Public Document Pack

To: All Members of the Policy and Resources Committee (and any other Members who may wish to attend)

J. Henshaw
LLB (Hons)
Clerk to the Authority

Tel: 0151 296 4000
Extn: 4112 Helen Peek

Your ref: Our ref HP/NP Date: 24 March 2014

Dear Sir/Madam,

You are invited to attend a meeting of the **POLICY AND RESOURCES COMMITTEE** to be held at **1.00 pm** on **TUESDAY, 1ST APRIL, 2014** in the Temporary Conference Room at Merseyside Fire and Rescue Service Headquarters, Bridle Road, Bootle.

Yours faithfully,

Clerk to the Authority

Encl.

This page is intentionally left blank

MERSEYSIDE FIRE AND RESCUE AUTHORITY

POLICY AND RESOURCES COMMITTEE

1 APRIL 2014

AGENDA

Members

Les Byrom (Chair)
Robbie Ayres
Roy Gladden
Ted Grannell
Steve Niblock
Denise Roberts
Sharon Sullivan
Pat Moloney
Anthony Boyle

1. Preliminary Matters

Members are requested to consider the identification of:

a) declarations of interest by individual Members in relation to any item of business on the Agenda

b) any additional items of business which the Chair has determined should be considered as matters of urgency; and

c) items of business which may require the exclusion of the press and public during consideration thereof because of the possibility of the disclosure of exempt information.

2. Minutes of the Previous Meeting (Pages 1 - 6)

The Minutes of the previous meeting of the Policy and Resources Committee, held on 14th January 2014, are submitted for approval as a correct record and for signature by the Chair.

3. Critical Incident Stress Management (Pages 7 - 14)

To consider Report CFO/040/14 of the Deputy Chief Fire Officer, concerning an update on the Critical Incident Stress Management Procedure; which was introduced to Merseyside Fire & Rescue Authority in July 2013.

4. **Access to Social Media** (Pages 15 - 28)

To consider Report CFO/031/14 of the Deputy Chief Executive, concerning approval for ICT to open up access to Social Media Sites on the Corporate network, for all Merseyside Fire & Rescue Authority staff.

5. **Access Audit Report and Recommendations for Estates work** (Pages 29 - 60)

To consider Report CFO/032/14 of the Deputy Chief Fire Officer, concerning a summary of the recent Access Audit carried out across 22 Stations.

6. **Protective Security Policy and related Service Instructions** (Pages 61 - 114)

To consider Report CFO/012/14 of the Deputy Chief Fire Officer, concerning the Policy and Service Instructions that have been developed to enable the Authority to implement the requirements of the Governments Protective Security Strategy.

7. **Review Of Improvement Scheme** (Pages 115 - 118)

To consider Report CFO/039/14 of the Deputy Chief Fire Officer, concerning progress and outcomes in relation to the Authority's Improvement Scheme.

8. **APPLICATION FOR EARLY RELEASE OF PENSION (DEFERRED) LGPS** (Pages 119 - 128)

To consider Report CFO/036/14 of the Chief Fire Officer, concerning an application for an early release of pension.

This Report contains EXEMPT information by virtue of Paragraph 1 of Part 1 of Schedule 12A of the Local Government Act 1972.

If any Members have queries, comments or require additional information relating to any item on the agenda please contact Committee Services and we will endeavour to provide the information you require for the meeting. Of course this does not affect the right of any

Member to raise questions in the meeting itself but it may assist Members in their consideration of an item if additional information is available.

Refreshments

Any Members attending on Authority business straight from work or for long periods of time, and require a sandwich, please contact Democratic Services, prior to your arrival, for arrangements to be made.

This page is intentionally left blank

MERSEYSIDE FIRE AND RESCUE AUTHORITY

14 JANUARY 2014

MINUTES

Present: **Cllr Leslie T. Byrom CBE (Chair)** Councillors Robbie Ayres, Dave Hanratty, Ted Grannell, Steve Niblock, Denise Roberts, Sharon Sullivan and Pat Moloney

Also Present: Boyle, Linda Maloney and Lesley Rennie

Apologies of absence were received from: Cllr Roy Gladden

1. Preliminary Matters

Members considered the identification of declarations of interest, any urgent additional items, and any business that may require the exclusion of the press and public.

Resolved that:

a) no declarations of interest were made by individual Members in relation to any item of business on the Agenda

b) The Chair determined that due to very short timescales given by government for consultation and the need to discuss with partners the approach to a shared response, that:

Item 7: Government Consultation on the Biding Process for 2015/16 Transformation Funds Report CFO/008/14, and;

Item 8: Local Government Finance Settlement 2014/15 Report CFO/009/14, be admitted onto the Agenda and consideration as additional urgent items of business.

c) The Following Items of business required the exclusion of the Press and Public:

Item 3: Part 2 of the Minutes of the previous meeting held on 19th November 2013, due to containing information Exempt by virtue of paragraph 3 of Part 1 of Schedule 12A of the Local Government Act 1972, and;

Item 6: Licences for the Playing of Music and Films Report CFO/005/14, due to containing exempt information by virtue of paragraph 3 of Part 1 of Schedule 12A of the Local Government Act 1972

2. Minutes of the Previous Meeting

The Minutes of the previous meeting of the Policy and Resources Committee, held on 19th November 2013, were approved as a correct record and signed accordingly by the Chair.

3. Part 2 - EXEMPT Minutes of the Previous Meeting

The Chair determined that Part 2 – Exempt Minutes of the previous meeting 19th November 2013 be considered following consideration of all open business on the Agenda. Therefore Item 3 was moved and considered after item 8.

The Minutes of the previous meeting of the Policy and Resources Committee held on 19th November 2013 were approved as a correct record and signed accordingly by the Chair.

4. Joint Control Centre Update

Members considered Report CFO/004/14 of the Deputy Chief Executive Officer, providing an update regarding progress of the work-streams associated with the Joint Command and Control Centre development including the Heritage Centre and related Workshops works, and forward look at key milestones to practical completion.

The opportunity to speak to contractors regarding any future slippage was discussed, and it was suggested that it be appropriate to bring a lessons learned report to a future Performance and Scrutiny Committee, and consider requesting the attendance of an appropriate representative from the contractors.

Members commented on the good development of the project and expressed appreciation to all staff involved in the project delivery.

Members welcome the completion of this major project and look forward to a tour of the new facilities once it is safe to do so.

Resolved that:

a) The report be noted;

b) Members considered the financial implications section of the report, and acknowledge the overall project cost rise from £11.4m to £11.7m due to some variations in requirements.

c) £163,000 of the Capital reserve established to cover unforeseen variations and manage associated risks of major capital projects, be allocated to cover the Merseyside Fire and Rescue Authority attributed costs.

d) Delegated power be granted to the Deputy Chief Executive Officer to approve any further minor variations required to the capital budget for finalised variations, in consultation with the Chair, and to fund these from the capital reserve that Members have set aside for this purpose.

5. Freedom of Information Requests

Members considered report CFO/001/14 of the Deputy Chief Fire Officer advising of the number of Freedom of Information requests received between 2011 and 2013.

It was noted that it would be useful to include an additional column in the table to categorise where requests had been received from the same individual/s to identify repeat requesters.

It was noted that some of the requests related to information which should be readily available, to which it was confirmed that where this as the case the requester was directed to where to locate the information.

Resolved that:

The report be noted

6. Licences for the Playing of Music and films

The Chair determined that due to the report containing Exempt information, Item 6: Licences for Playing Music and Films be considered after item 3 – which follows item 8 of the Agenda, with the exclusion of the press and public.

Members considered report CFO/005/14 of the Clerk to the Authority, concerning the requirements for licences for playing of music and films on Fire and Rescue Authority premises.

Considerable debate took place in the form of Members distaste against the right to charge a Public Service, along with other businesses and charitable organisations, for the playing of music and films on premises, and possible ways around such costs which equate to 1 Firefighter post per year.

Members were advised by the Clerk to pay the licences, as to not do so would be unlawful.

Resolved that:

After much debate The Chair moved that:

a) Members agree to comply with the law and meet legal obligations;

b) Officers be authorised to continue to look into negotiations with licencing organisations to reduce licence costs;

c) The budget be aligned for 2014/15 to allow for payment of licences ;

d) The Authority lobby Ministers, with other Fire and Rescue Authorities and public bodies, to seek recognition that budgets have been pressed, and such Licences should not be applicable, and request that it be included on the LGA agenda.

Unanimously agreed by Members.

7. Government Consultation on the Bidding Process for 2015/16 Transformation Funds

Members considered report CFO/008/14 of the Deputy Chief Executive Officer regarding the proposed response from Merseyside Fire and Rescue Authority to Government in relation to consultation on the bidding process for 2015/16 Transformation Funds.

This was accepted on to the agenda as an urgent item due to very short timescales given by government for consultation and the need to discuss with partners the approach to a shared response.

Resolved that:

a) The report be noted, and;

b) The proposed response be approved.

8. Local Government Finance Settlement 2014/15

Members considered report CFO/009/14 of the Deputy Chief Executive Officer regarding the proposed response from Merseyside Fire and Rescue Authority in relation to the Local Government Finance Settlement 2014/15.

This report was accepted on to the agenda as an urgent item due to very short timescales given by government for consultation and the need to discuss with partners the approach to a shared response.

Resolved that:

a) The report be noted, and

b) The draft response be approved.

Close

Date of next meeting Tuesday, 1 April 2014

This page is intentionally left blank

MERSEYSIDE FIRE AND RESCUE AUTHORITY			
MEETING OF THE:	**POLICY AND RESOURCES COMMITTEE**		
DATE:	**1 APRIL 2014**	**REPORT NO:**	**CFO/040/14**
PRESENTING OFFICER	**DEPUTY CHIEF FIRE OFFICER**		
RESPONSIBLE OFFICER:	**NICK MERNOCK – DIRECTOR OF PEOPLE & ORGANISATIONAL DEVELOPMENT**	**REPORT AUTHOR:**	**KELLY PATTERSON-SENIOR OCCUPATIONAL HEALTH OFFICER**
OFFICERS CONSULTED:	**Paul Blanchard-Flett (Occupational Health Manager), John McNeil (Health and Safety Manager), SM Thomas (Operational Performance Team)**		
TITLE OF REPORT:	**CRITICAL INCIDENT STRESS MANAGEMENT**		

APPENDICES	**NONE**

Purpose of Report

1. To update Members on the Critical Incident Stress Management procedure; which was introduced to Merseyside Fire and Rescue Authority (MF&RA) in July 2013.

Recommendation

2. That Members note the contents of this report.

Executive summary

3. In August 2012 a critical incident working group was formed to review the mental health needs of fire and rescue authority employees throughout their career, from entry to exit, with particular reference to the mental health impact following exposure to critical incidents throughout their service. The group were tasked to research and report, with recommendations an implementation plan for the Service.

4. The contents of this report are intended to provide an update to members following the launch of the Critical Incident Stress Management procedure which was introduced within MF&RA in July 2013

Introduction and Background

5. After extensive research and reflecting on other UK Fire and Rescue Service support systems already in place post-attendance at serious and potentially

traumatic incidents, the Service adopted a Critical Incident Stress Management (CISM) process. Effective management of staff exposed to potentially traumatic stress at incidents is a recommendation under Sec.13 Fire and Rescue Service Health, Safety and Welfare Framework 2012 document.

6. Following a scoping exercise to establish Organisational and Individual requirements, recommendations were presented to the Health, Safety and Welfare committee and SMG, and as a result, a Critical Incident Stress Management procedure was introduced in to MF&RA in July 2013.

7. The Critical Incident Stress Management procedure provides a response to critical incidents, as well as promoting an understanding and developing a framework for the individual or team to manage any reactions encountered following attendance at or exposure to a potentially traumatic incident.

8. Critical Incident Stress Management involves a three tier response consisting of defusing, debriefing and bridging team support.

9. Trained Defusing Officers undertake the initial response; Defusing is conducted immediately when staff have returned to their station or normal workplace location following attendance at a critical incident - always before they go off duty.

10. To enable crews to be defused post incident the Authority required defusing officers to be appointed and trained. Due to the nature of the incidents it was decided that the Station Manager (SM) group would be appointed as defusing officers because:

    a) SMs would attend all of the incidents that may be deemed traumatic/critical
    b) SMs by nature of their command role would generally be remote from any potential trauma at scene and therefore able to make a more informed assessment of heightened emotions of crew members

11. All SM's have now been trained as defusing officers. This training is delivered by the Critical Incident Coordinators who have received enhanced Critical Incident Stress Management debriefing and defusing training utilising the Organisation LivewellWorkWell.

12. Debriefing Officers conduct the second stage of the process. If a full Critical Incident debrief is required after the defusing stage (based on the nature of the incident and the decision of the defusing officer), Debriefing Officers will hold a structured meeting with those involved, enabling all attending individuals to share their experiences of the incident, reviewing facts, feelings and reactions encountered. This should take place within 48-72 hours following the incident. When this is not possible it will take place as soon as staff return to duty after this time.

13. A selection process was held for all Service personnel to apply to become Debriefing Officers. After receiving a substantial amount of applicants 15 were selected. This 15 included staff from uniformed and non-uniformed posts at

every level within the Organisation including Firefighters, Managers, Advocates and Support Staff.

14. Debriefing Officers received an intensive three day course to attain the required standard. The course was delivered by LiveWellWorkWell.

15. Bridging team support is offered to all personnel following the debriefing process. The Bridging Team consists of a range of voluntary personnel, uniformed and non-uniformed (religious and non-religious), under the leadership and direction of the Authority Chaplain.

16. A dedicated intranet portal site has been created and developed. This site enables Service personnel to view CISM information and is also used by Coordinators to monitor and evaluate progress following defusing and debriefing.

Progress to Date

17. Since going live in July 2013 there have been 22 critical incidents declared– all have been as a result of an Operational Incident.

18. Three of these 22 incidents subsequently led to a full critical incident debrief being arranged.

19. There has been one critical incident declared at MACC and subsequent defusing was undertaken with the MACC Operators.

20. All Authority staff are in the process of receiving a Critical Incident Stress Management presentation to ensure that they are familiar with the process .These presentations are being delivered to each individual watch and team within the Service, the rationale being that smaller groups are more interactive and more likely to engage with the individual delivering the presentation. Presentations are delivered by Debriefers and currently 53 of these presentations have been completed.

21. Critical incident coordinators have received both constructive and positive feedback from various sources including: Crews, Defusing Officers, Debriefing Officers and Bridging Team members.

22. One of the most common comments fed back to the coordinators following the CISM presentations from Crews is that the procedure is ‘the right thing to do’ and that ‘it is long overdue’. It has also been highlighted in operational debriefing forms as an area of good practice post-incident.

23. Some initial issues have been highlighted regarding the debrief coordination. It has not always been possible that everyone who attended the critical incident has been able to attend the critical incident debrief- due to detached duties, annual leave etc. Coordinators have been able in such instances to make individual contact to offer one-to-one post incident support.

24. An incident with Whiston station highlighted the practicalities of defusing always occurring on return to station after a critical incident. The incident happened at

the end of shift and crews wanted to go home rather than be defused. Levels of engagement with the process is paramount and so where defusing should always take place before crews finish shift, defusing in this instance should be judged on the expected levels of engagement. Defusers are encouraged to seek the advice of the coordinators before allowing crews to leave shift before defusing occurs.

25. Learning points were highlighted following a recent incident at Speke. Contrary to the procedure, crews were grouped together rather than being defused at their own locations. This led to a lack of engagement with defusing officers. Although in this particular incident the desired outcome was slightly compromised, crews still reported back that they recognised that the Service was attempting to do the right thing by its crews.

Future considerations

26. The coordinators aim to ensure that all CISM presentations are delivered to all staff, to ensure that all personnel are aware of and understand the procedure and are given the opportunity to feedback any comments.

27. A development day for the Debriefers has been conducted since the initial training to refresh their knowledge and skills. Training will be offered to those involved in the CISM procedure as and when deemed required.

28. It may be possible to consider in the future sharing training with neighbouring Fire and Rescue Authorities such as Greater Manchester and Cumbria with who use the CISM procedure and the same Organisation LiveWellWorkWell for training.

29. The Coordinators who conduct the defuser training have now trained all SM's in defusing. Defuser training is now planned for the Watch Managers within the Search and Rescue Team (SRT), for instances when they may be deployed to other areas of the country where a SM may not be present to conduct defusing. As an aspiration, all Watch Managers within MF&RA will be fully trained in defusing.

30. All bridging team members are required to be qualified to a minimum of Mental Health First Aid (2 day course). All defusing and debriefing officers are strongly encouraged also to undertake the Mental Health First Aid course. This training is now being undertaken by the MF&RA Mental Health First Aid Instructor.

31. Mental Health First Aid Lite (1/2 day course) which is a brief mental health awareness course is intended to be delivered to all MF&RA personnel in the near future. This will be delivered by the MF&RA Mental Health First Aid trainer.

32. The CISM Coordinators following feedback from crews have had discussions regarding the creation of a Memorandum of Understanding between MF&RA and local hospitals/groups so that a nominated MF&RA person may contact the local hospital after critical incidents for updates on the casualties involved. This

is hoped that this may assist MF&RA crews who attended the incident with some closure.

33. Occupational Health notice boards across all stations may be considered to be useful in order to promote the services of Occupational Health, the welfare support available, monthly health promotions and critical incident support/procedural information.

34. Developing workforce understanding of the Bridging Team will be promoted in the near future once the team is fully established and trained in Mental Health First Aid.

35. Critical Incident Coordinators will present updates regarding this report to SMG and elected members following the ongoing review of the critical incident stress management procedure.

Equality and Diversity Implications

36. An Equality Impact Assessment (EIA) was completed at the initial implementation of the Critical Incident Stress Management procedure. This procedure continues to apply to all employees of MF&RA and does not exclude any group or individual.

Staff Implications

37. The implementation of the Critical Incident Stress Management process will support and promote mental wellbeing in the workplace. The introduction of this process aims to reduce absence from issues that negatively affect the welfare of staff.

38. Commitment will be required from Senior Management to allow staff time to attend the relevant training courses for this process to proceed.

Legal Implications

39. Critical Incident Stress Management will ensure that the Authority complies with its duties under the Health and Safety at Work Act 1974 (s.2); by ensuring that the Authority is acting reasonably practical in its attempts to reduce stress in the workplace. By using this procedure, the Authority is demonstrating compliance with CFOA guidance “Health, Safety and Welfare Framework Document 2012 (s.13) and Management of Health and Safety at Work Regulations 1995 Regulation. 6.

Financial Implications & Value for Money

40. Training costs to date have included:

Defusing Officers – £1,583 for the train the trainer course in defusing. These two individuals are Critical Incident Stress Management Coordinators and are existing employees from Occupational Health and Operational Response.

Defusing training is then delivered free of charge to defusing officers.

Debriefing Officers - Debriefers are now fully qualified in Critical Incident Stress Management. This is following completion of a 3 day course run by LiveWellWorkWell at a cost of £4516. This cost also included a review and development day and access for a period of 12 months following initial training to a 24/7, 365 days a year 'debriefer helpline'.

The overall cost for the training is £6,100.

41. The Service approached a Health and Safety software management company to arrange recording and monitoring of the procedure (i.e. enabling a vehicle to report back attendance at Critical Incidents and debriefs by personnel). The final cost for this product was quoted at £30,000. Coordinators viewed this as excessive and requested an employee within the Strategy and Performance department to review the requirements. This employee was able to create a product using existing Intranet Portal Systems and software to create a system that was to the exact specification required,.

42. A Mental Health First Aid instructor is readily available within the Service; cost for training is limited to the cost of the manuals and workbooks at the current price of £25 per person. CIPD Survey October 2011 states that stress has become the most common cause of long term absence for manual and non-manual employees and on the basis of these figures, The National Association for Mental Health (MIND) recommends that with a greater awareness and mental health support that nationally businesses could save £8 billion per year.

43. The introduction of this procedure aims to reduce the instances of stress, days lost due to stress related illnesses and the associated costs. As this is a new procedure there has been insufficient time to highlight any financial evidence of monetary savings to MF&RA regarding stress related absences. However, given a suitable period of time, this should be something in which may be observed in the future.

44. Finance is provided through existing Occupational Health Services budgets.

Risk Management, Health & Safety, and Environmental Implications

45. The leads on the project presented their research to the Health, Safety and Welfare committee. After reviewing and discussing the findings, the committee agreed that Critical Incident Stress Management was the best way forward for MF&RA as opposed to alternative options.
Regular updates have been reported back to the committee.

46. There are no environmental implications relating to this process.

Contribution to Our Mission: *Safer Stronger Communities – Safe Effective Firefighters*

47. The introduction of the critical incident stress management process directly supports all Service staff in their mental wellbeing and contributes to making firefighters safer and therefore more effective in their duties

BACKGROUND PAPERS

	Fire Service Health, Safety and Welfare Framework 2012 Document
CFO/045/13	Critical Incident Stress Management SMG Report
	Critical Incident Stress Management scoping group document
	Service Instruction 0789 CISM

GLOSSARY

This page is intentionally left blank

MERSEYSIDE FIRE AND RESCUE AUTHORITY			
MEETING OF THE:	**POLICY AND RESOURCES COMMITEE**		
DATE:	**1ST APRIL 2014**	**REPORT NO:**	**CFO/031/14**
PRESENTING OFFICER	**KIERAN TIMMINS DEPUTY DEPURTY CHIEF EXECUTIVE**		
RESPONSIBLE OFFICER:	**KIERAN TIMMINS HEAD OF TECHNOLOGY**	**REPORT AUTHOR:**	**ED FRANKLIN**
OFFICERS CONSULTED:	**RIA GROVES – TRAINEE SOLICITOR PETER RUSHTON – DIRECTOR OF CORPORATE COMMUNICATIONS NICK MERNOCK – DIRECTOR OF PEOPLE & ORGANISATIONAL DEVELOPMENT DEB APPLETON – DIRECTOR OF STRATEGY & PERFORMANCE**		
TITLE OF REPORT:	**ACCESS TO SOCIAL MEDIA**		

APPENDICES:	**APPENDIX A**	**SI0699 – USING SOCIAL MEDIA**

Purpose of Report

1. To request authority approval for ICT to open up access to Social Media Sites on the corporate network for all Merseyside Fire & Rescue Service (MFRS) staff.

Recommendation

2. That Members;

a)Note recent upgrade of Websense, the corporate Web Filtering and Email filtering solution

b)Approve the access to Social Media on the Corporate ICT Network for all staff

c) Note the mitigation measures in place to avoid abuse or misuse

Out Comes of Using Social Media

- Promote Merseyside Fire & Rescue Authority (MF&RA) Corporate Communications Strategy
- Promote and deliver MF&RA work and the positive outcomes in and to our community

- Using social media in the work place not just for staff to stay in touch with family and friends but to be more productive and effective in their work

- Connecting and maintaining relationships with other fire and rescue services and partners

Introduction and Background

3. Social media is the name commonly given to Interactive Communication Technology websites; primarily those which enable users to interact and communicate by sharing content such as opinion, media (video, images and audio), knowledge and interests.

4. Typically, social media contributes to the building of 'networks' or online communities while encouraging participation and engagement. The term encompasses many variations of online media. Examples include blogs, micro-blogs (Twitter), podcasts, 'wikis' (such as Wikipedia), message boards, social book marking websites (Reddit), social networking websites (Facebook, MySpace) and media content sharing websites (such as Flickr, YouTube).

5. Corporate Communications have access to Facebook and Twitter and they are responsible for the Merseyside Fire & Rescue Service (MFRS) presence in the Social Media Community. There are pockets of social media activity by various departments such as Youth Engagement.

6. The Authority has in place an ICT Acceptable Usage Policy (ICTPOL03) which covers a number of Service Instructions (SI) including the SI relevant to this report, SI0699 Using Social Media.

7. This SI will ensure that all MFRS personnel recognise the importance of new and emerging media platforms for communicating and consulting with the public, whilst engaging in these new methods of communication in a responsible, coordinated and consistent manner.

8. The corporate Web Filtering and Email filtering solution for staff accessing the internet on their MF&RA computer is the Websense system.

9. Websense has in built management reporting of user activity and statistics which are presented to Level 6 Budget Managers on a monthly basis via the ICT Infrastructure Report.

10. In the past Websense only offered complete granular control of all corporate access to the internet and email. This control has now been extended to Social Media sites in the latest available upgrade.

11. The upgrade version of Websense has been successfully completed

<u>Actions to be taken</u>

12. If open access is approved continue with this action list.

13. Progress the Service Instruction 'SI0699 Using Social Media' through consultation process estimated at 21 days.

14. When in place send a communication out to all staff including highlighting the Social Media SI.

15. Action a simple change to the Websense configuration opening up Social Media to all staff on the Corporate Network

16. ICT will amend the ICT Infrastructure Usage report to include user activity & statistics in the area of social media. This is made available to Level 6 Budget Managers.

17. MF&RS staff must comply with SI0699 Using Social Media Policy and will continue to work closely with and seek permission from Corporate Communications to ensure any future Social Media initiatives are aligned to the Corporate Strategy.

Equality and Diversity Implications

18. This initiative has a positive impact for all Equality Groups with no perceived negative concerns. Consultation with the Equality and Diversity Consultation Manager has ascertained there is no requirement to produce a full Equality Impact Assessment (EIA).

Staff Implications

19. Advantages of allowing the use of social media at work:

- Improved efficiency and productivity.
- Increased Loyalty.
- Improved Employee Satisfaction.
- Attracting the right kind of talent. Generation X and Y individuals.
- Workplace Harmony
- Managers can manage staff usage supported by, amongst other controls, the Infrastructure Usage Report

20. Dis-advantages of allowing the use of social media at work:

- Employees can waste time
- Detracts from their normal jobs
- Companies can be portrayed in a bad light by a negative employee
- Decreases productivity

Legal Implications

21. The use of social media does not come without legal implications for any business or individual.

22. The biggest risk to an employer is the improper use of public electronic communications networks by employees. In particular the risk the Authority may be exposed to through use of social media is breaches of the Data Protection Act and Defamation actions committed by employees.

23. There are also serious risks to be considered in respect of the Regulation of Investigatory Powers Act 2000 (RIPA) whereby surveillance may deliberately or accidently take place. For example the Facebook page or Twitter account of a particular individual could be being monitored for purposes of preventing or detecting crime. This would be described as covert surveillance in many circumstances and although it may be inadvertent, it must be authorised via RIPA procedures before it can take place to ensure that such surveillance is proportionate and does not unnecessarily breach Human Rights.

24. Although surveillance of employees for legitimate purposes does not technically fall under RIPA, it must nevertheless be authorised by an alternative route to ensure that Human Rights are properly considered and protected and that there is accountability and an audit trial of decisions.

25. The Clerk to the Authority is able to advise any employee of the correct approach to authorisation or both employees and non-employees

26. Additionally criminal activities that may be carried out by employees whilst at work such as online harassment, public disorder offences (threats made against another individual on a website, forum or social network that will be seen by the intended target) and incitement of racial hatred online present a real reputational risk to the Authority or may even hold the Authority to be vicariously liable if such activities have been carried out during their employment and as a representative of the Authority.

27. However as these risks to the Authority are already present through any employees use of social media outside of work hours implementing social media access within Authority premises will not greatly increase the risks referred to above particularly if the social media policy addresses the way in which sites are used (for example social media is only accessed in employees own time such as their lunch break) and there are rules of engagement with social media users, monitoring of channels and employees communication(for example uploading of videos of confidential data at work).

Financial Implications & Value for Money

28. This initiative is possible due to the software upgrade of Websense the cost of which was covered within the ICT current budget.

Risk Management, Health & Safety, and Environmental Implications

29. The main risk of using social media as an organisation would be the potential damage to reputation due to misuse.

30. There is also the risk of damage to an individual's personal and/or professional reputation.

31. Social Networks are having a greater risk of exposing the organisation to virus and malware threats. This is because users place too much trust in people within their social network, even though they may not know the people in real life. Consequently users are more likely to click on a link within Twitter, Facebook or LinkedIn than in an email, where most people today are a little more circumspect.

32. Tools such as Websense, however, are becoming more sophisticated in protecting the Corporate ICT Infrastructure from such risks.

Contribution to Our Mission: *Safer Stronger Communities – Safe Effective Firefighters*

33. Use of Social media will make a positive difference to the community of Merseyside and enable our people to be the best they can be.

BACKGROUND PAPERS

20/10/2013 Re-issue of previous SMG Report with newly attached Service Instruction

GLOSSARY OF TERMS

EIA	Equality Impact Assessment
ICT	Information and Communication Technology
MFRA	Merseyside Fire and Rescue Authority
MFRS	Merseyside Fire and Rescue Service is the service provided by MFRA.
POD	People and Organisational Development
SI	Service Instruction

This page is intentionally left blank

"An Excellent Authority"

Service Instruction 0699
Using Social Media

Document Control

Description and Purpose

This document is intended to give guidance to all MF&RS Staff about using social media (for example Twitter and Facebook) for both professional and personal use.

Active date	Review date	Author	Editor	Publisher
01/04/2011	24/05/2014	Ed Franklin	Ed Franklin	Sue Coker

Permanent	X	Temporary		If temporary, review date must be 3 months or less.

Amendment History

Version	Date	Reasons for Change	Amended by
1.1	26/04/2012	Document Control Update Following Annual Review	B. Kenny
1.2	22/05/2012	Document Control Update Following Annual Review	B. Kenny
1.3	20/11/2013	Update Prior to Opening Up Social Media Access Decision	B. Kenny/R. Groves

Risk Assessment (if applicable)

Date Completed	Review Date	Assessed by	Document location	Verified by(H&S)

Equalities Impact Assessment

Initial	Full	Date	Reviewed by	Document location
	X	14/04/2010		

Civil Contingencies Impact Assessment (if applicable)

Date	Assessed by	Document location

Related Documents

Doc. Type	Ref. No.	Title	Document location
Policy	ICTPOL03	ICT Acceptable Use Policy	Portal
Policy	STRPOL09	Information Governance and Security Policy	Portal
SI	SI0703	Internet Access and Usage	Portal

Contact

Department	Email	Telephone ext.
ICT	edfranklin@merseyfire.gov.uk	4569

Target audience

All MFS	X	Ops Crews		Fire safety		Community FS			
Principal officers		Senior officers		Non uniformed					

Relevant legislation (if any)

The Obscene Publications Act	1964
The Protection of Children's Act	1999
The Video Recordings Act	2010
Copyright, Designs and Patents Act	1988
Malicious Communications Act	1988
The Computer Misuse Act	1990
Trade Marks Act	1994
The Data Protection Act	1998
Communications Act	2003
The Regulation of Investigatory Powers Act	2000

USING SOCIAL MEDIA INTRODUCTION

Purpose and Scope

This Service Instruction (SI) is intended to assist Merseyside Fire & Rescue Authority (MFRA) employees in adopting appropriate conduct when using social media..

The use of social media is evolving and MFRA as an organisation are aiming to join this media platform in order to promote MFRA's corporate aims and work undertaken with the community and other local authority partners.

The SI will outline the expectations MFRA require from employees with regard to social media use and the actions taken in consequence of breaching this SI.

Defining Social Media

Social media is the name commonly given to Interactive Communication Technology websites; primarily those which enable users to interact and communicate by sharing content such as opinion, media (video, images and audio), knowledge and interests.

Typically, social media contributes to the building of 'networks' or online communities while encouraging participation and engagement. The term encompasses many variations of online media. Examples include blogs, micro-blogs (Twitter), podcasts, 'wikis' (such as Wikipedia), message boards, social book marking websites (Reddit), social networking websites (Facebook, MySpace) and media content sharing websites (such as Flickr, YouTube).

The paramount feature of all of these platforms is that of a central focus on User Generated Content, whether it is a photograph stream on Flickr or a Poll on Facebook, they also facilitate conversations and online interactions between groups of people.

Rules and Guidance for Social Media Use by MFRA Employees

When publishing content (posting, uploading, sharing) on social media it is important to be aware that you have no legal right to privacy and will be held accountable for the content published. Be mindful that it can remain published for many years.

Do not allow any other persons to access your social media identities. You will be bound by your social media account and therefore accountable for whatever content is published through it.

Never divulge your user-id or password to anyone else. Under no circumstances should passwords be written down and left in an un-secure or non-private area.

You must ensure that you read and comply with any social media's terms and conditions

Do not upload, post, forward (including links) any abusive, obscene, discriminatory, harassing, derogatory or defamatory content.

Abuse or harassment of any employee will not be tolerated. Never use social media to intimidate, bully or in any way attack or abuse colleagues or members of the community. Any MFRA employee who feels they have been harassed, bullied or offended by content posted on social media by a colleague should contact their line manager or Professional Standards to report the incident.

Ensure that you clearly identify yourself in any social media use, write in the first person and ensure that there is a clear statement that the views you express are not any reflection on the views held by MFRA when identifying yourself as an MFRA employee, or discussing the organisation,

Don't discuss or reference other colleagues, partners or contractors without their explicit approval. Do not monitor anyone else's content or account information as a means of providing evidence or criminal or disciplinary related conduct or for any other means. This will be deemed to be surveillance under the definitions contained in the Regulation of Investigatory Powers Act 2000. Any such monitoring must be properly authorised.

Do not upload post or forward any content belonging to a third party unless the third parties have given their consent. Prior to posting or uploading a link to a third party website ensure their terms and conditions permit such actions and ensure that it is clear to the user that they will move to a third parties website.

Never disclose any commercially sensitive, private or confidential information that is linked in any way to MFRA or MFRA employees.

Be open and honest when using social media whilst remaining aware of the impact your use might make on people's perceptions on MFRA as an organisation and respect others privacy when discussing topics.

Do not post, forward, forward or post a link to chain mail, junk mail or gossip

Never publish anything you are not comfortable with, always discuss it with your line manager if in any doubt.

Avoid publishing your contact details where they can be accessed and used widely by people you did not intend on viewing them and never publish anyone else's contact details.

If you notice any content posted on social media websites about MFRA either complementary or critical please report to your line manager.

Enquiries or requests for information from social media, including requests from bloggers, should be immediately forwarded to the Corporate Communications Team (corporatecommunications@merseyfire.gov.uk) for a response. Employees must not respond directly to such enquiries without express permission from the Corporate Communications.

MFRA Social Media Accounts

Only Corporate Communications are permitted to post material on a social media website in the name of and on behalf of MFRA. This is to ensure all content posted online is consistent with the corporate aims, core and personal values. Also, that it complements, and does not conflict, with information already being communicated across traditional media platforms.

If an employee requires the use of MFRA's social media accounts in order to promote or highlight work undertaken for the community or as part of any other partnership with outside organisation a request must be made to Corporate Communication. The request will be reviewed accordingly.

Any station or department that requires information to be disseminated via the social media platforms must contact Corporate Communications who will advise appropriately.

Personal Use of Social Media on MFRA Premises

MFRA permit incidental use of social media websites subject to the use being minimal and being conducted substantially out of work hours (lunch break is defined as out of work hours). This extends to personal mobile devices.

Any social media use must not interfere with MFRA work or office commitments

Any social media use must comply with this SI and any other relevant policy or service instruction including but not limited to Equality and Diversity Policy, Bullying and Harassment Policy, Data Protection Policy and Disciplinary Procedure.

Activity on social media websites during office hours should complement and or support your role within MFRA and should be used in moderation

The permitted use of social media is a discretionary privilege, not a right and this privilege should not be abused or overused. MFRA retains the right to withdraw this privilege at any time.

Monitoring Use of Social Media Websites

All use of social media websites, irrelevant whether it has been accessed for work related purposes may be monitored if breaches of this service instruction are evident. Action may also be taken in accordance with the Disciplinary Procedure.

MFRA reserve the right to restrict or prevent access to specific social media websites if it has been deemed the personal use is excessive. Monitoring will only be exercised to the extent the law permits and is justifiable for business purposes.

Any misuse of social media can constitute a criminal offence or in certain circumstances may give rise to criminal (or even civil) liability against yourself and/or MFRA This may affect MFRA's reputation and damage the relationship with the community.

Certain actions on social media websites whether in a professional or personal capacity can amount to gross misconduct including but not limited to the uploading, posting, forwarding or posting a link to any material that is explicit (i.e. pornographic), invades the privacy of others, false or defamatory statements about any individual or organisation, material which is offensive, obscene, abusive, criminal discriminatory, breaches any Court Order or rule of law, breaches copyright or other intellectual property rights, derogatory or which may cause embarrassment or risk the reputation of MFRA, MFRA employees, partners or the community

Some actions such as monitoring anyone else's content or account information as a means of providing evidence of criminal or disciplinary related conduct or for any other means will be deemed to be surveillance under the definitions contained in the Regulation of Investigatory Powers Act 2000. Any such monitoring must be properly authorised.

There are clear procedures for obtaining authorisations for both employee and non-employee surveillance. This information is all contained on the Legal Services page of the Portal however the Clerk to the Authority can advise any employee of the procedures and requirements around this legislation. The important thing is that surveillance whether intended or otherwise is unlawful without the correct authorisations being in place as peoples' human rights must be protected in law.

Any misuse of social by any employees of MFRA should be reported to your line manager.

Any evidence of misuse of the social media found may result in an investigation being undertaken in accordance with MFRA's Disciplinary Procedure and details of the monitoring records may be disclosed to the investigation officers and any other relevant persons. Any such information may also be provided to the police in connections with any criminal investigation.

Any breach will be addressed under the Disciplinary Procedure and action taken accordingly. Please note if warranted discipline may result in a summarily dismissal.

Roles and Responsibilities

User:

You must ensure that you read and comply with this instruction

Line Management:

The monthly Infrastructure Usage report distributed by the ICT Service Delivery Manager to Level 6 Budget Holders should be reviewed for unauthorised, inappropriate or excessive use; serious or repeated breach of this Instruction, or any other form of use potentially damaging to the Authority; and arrange for it to be investigated by requesting individuals usage reports via the ICT Service Delivery Manager

ICT Service Delivery Manager:

It is the responsibility of the ICT Service Delivery Manager to:

Ensure that the contents of this instruction is published on the portal and understood by all members of MFRA
Provide individual usage reports to Line Management when requested
Inform Professional Standards when individual usage reports are requested
Review this Service Instruction on a regular basis and communicate amendments/additions

This page is intentionally left blank

MERSEYSIDE FIRE AND RESCUE AUTHORITY			
MEETING OF THE:	**POLICY AND RESOURCES COMMITTEE**		
DATE:	**1ST APRIL 2014**	**REPORT NO:**	**CFO/032/14**
PRESENTING OFFICER	**DEPUTY CHIEF FIRE OFFICER**		
RESPONSIBLE OFFICER:	**DEB APPLETON**	**REPORT AUTHOR:**	**WENDY KENYON**
OFFICERS CONSULTED:	**WENDY KENYON STEWART WOODS STRATEGIC EQUALITY MEMBERS**		
TITLE OF REPORT:	**ACCESS AUDIT REPORT AND RECOMMENDATIONS FOR ESTATES WORK**		

APPENDICES:	**APPENDIX 1:**	**ACCESS AUDIT SUMMARY**
	APPENDIX 2:	**ACCESS AUDIT COST BY PRIORITY & DISTRICT**
	APPENDIX 3:	**COST SUMMARY BY TYPE**
	APPENDIX 4:	**AUDIT COST SCHEDULE -2013**
	APPENDIX 5:	**ACCESS AUDIT – KIRKBY STATION.**
	APPENDIX 6:	**PROPOSED SCHEDULE OF PRIORITY 1 AND FEMALE FF WORK TO BE CARRIED OUT**

Purpose of Report

1. To provide Members with a brief summary of the recent Access Audits carried out across 22 Stations and to provide Members with the necessary information for decisions to be made about what improvement work should be completed, by when and at what cost.

Recommendation

2. That Members;

a) approve the work required to make improvements for Female Firefighter facilities (changing and washing facilities) as highlighted in Appendices 1, 2 & 3, starting with those stations that currently have female Firefighters in post. This work is deemed a priority to be completed commencing April 2014

b) approve the Priority 1 work highlighted in Appendix 6 which also lists the recommended phasing for works across stations. This work is deemed to be a priority for 2014/15 estates work streams.

c) approve specific additional work recommended from Priority 2,3 and 4 as deemed appropriate by Estates Manager (e.g. Signage) highlighted in Appendix 2

d) note that costs are budgeted figures (already contained within existing budgets) based on industry guides and best value will be obtained in accordance with MFRS standing orders.

e) agree that ongoing monitoring of the access audit work will be reported by the Estates

Manager as part of the Estates Equality and Diversity action plan quarterly progress report, discussed at Strategic Equality Group meetings.

Introduction and Background

3. This report provides a summary of the 22 Access audit reports produced by David Trowler Associates and provides recommendations on the priorities for work to be completed. The Access audit report is summarised in the following documents:

- **Appendix 1** Overall Access Summary report for 22 stations audited showing what is accessible in relation to :
  - Public enquiries access
  - Safe Haven access
  - Meeting room access
  - Female Firefighter facilities
  - Corporate signage
  - Access to the building, Internal circulation, toilets, employee facilities and communal facilities

- **Appendix 2** provides an overall Summary of the priorities for access improvement and costs. The priorities are as follows:
  - **Priority 1** – Work required to ensure the services are accessible to the public. These are improvements that will assist in complying with Equality Act 2010 (essential)
  - **Priority 2 -** Improvements to overcome problems with existing site/building which would be beneficial to users with impairment, but not required by Equality Act 2010 (improvement)
  - **Priority 3** – Recommendations considered best practice or to suit a potential future employee. Best practice is considered to be work that is not required to fulfil a statutory duty but which would bring the item/area concerned up to a modern standard with regard to access /facilities
  - **Priority 4 -** Recommendations affecting accommodation only used by operational personnel.
  - **Recommendations about Facilities for Female Firefighters**- Operational only
- **Appendix 3** provides an overall cost summary by access type

- **Appendix 4** provides information on the standardised costing schedule

- **Appendix 5** gives an example of a full access audit report for information purposes only (Kirkby fire station)

- **Appendix 6** is a revised schedule of Priority **1** works using a number of weightings to establish the overall importance and priority for works required. Consideration has been given to the following :

  - Whether the station is one of the 10 Key stations

- Whether the station is in a district with limited up to date community facilities
- Whether the Station is likely to be subject to Merger or Closures
- Utilisation of station for partnerships and community work

4. No PFI stations have been audited as access for all was an integral part of the design of these new community fire stations. Not only do the PFI designs comply with legislative requirements for accessibility, they embody the spirit of inclusion, helping the Service in its goal to attract a more inclusive workforce and engage with the entire community, including hard-to-reach groups.

5. PFI Stations have been included in the attached summary reports only to highlight districts which have fully complaint PFI stations within them.

6. The standardised audit cost schedule has been produced in line with industry 'rule of thumb guides' and is for budget purposes only. Best value will be obtained in accordance with MFRS standing orders.

7. The government has announced yet further funding cuts for 2015/16 and intends to continue cutting beyond this. The current forecast is that the Authority will face a significant deficit. The Estates strategy document has highlighted and Authority Members have already approved in principle, the working up of a feasibility studies for station mergers. Works resulting from the access audits should be scheduled taking cognizance of these feasibility studies and the volume of community use at each station.

8. An access audit is being arranged for the JCC / SHQ refurbishment project to ensure that the building is assessed for access to achieve the same standard as all other buildings/stations. Outcomes of the report will be shared with SMG members in due course

9. Any new requests for community groups to access stations that require priority 1 access works to take place will be monitored and discussed with Diversity Consultation Manager and District Managers on a case by case basis, until all stations are fully accessible.

10. District Managers will be given electronic copies of the access audits for their Districts to help manage their community usage on stations that require access work.

Equality and Diversity Implications

11. Access Audits are positive in relation to Equality and Diversity as they help to improve our understanding about the issues that the disabled community may face when accessing our buildings and services. It has also considered the needs of Female Firefighters in relation to basic washing, sleeping and changing facilities.

Staff Implications

12. The impact of the Access Audit work will be positive on staff across the Service as buildings and stations will be upgraded to make them more accessible, especially for Disabled staff and Female Firefighters.

Legal Implications

13. The Equality Act 2010 makes clear that public organisations should review their services in relation to the needs of the 9 protected groups (Age, Disability, Gender, Race, Religion& Belief, Transgender, Sexual Orientation, Marriage and Civil Partnerships, Sex/Gender and Pregnancy and Maternity). This also includes access arrangements to community based services. The Access Audit helps to assess access to those buildings and services for Disabled people.

14. Please note that the Audit report refers to DDA (Disability Discrimination Act) which has been superseded by the Equality Act 2010.

Financial Implications & Value for Money

15. The current 5 year capital budget has a provision of £139,000 for Equality Act works, £89,000 for 13/14 with the remaining £50,000 over the period 2013/14 to 2017/18.

16. A reserve of £510,000 for Equality Act works was approved in CFO/080/13 from the under spend in Year End 2012/13.

17. Whilst no major capital refurbishments have been planned until feasibility studies are completed, a small scale works capital budget was approved to improve fire-fighter and community facilities. £500,000 of the capital investment reserve was set aside to support these works.

Risk Management, Health & Safety, and Environmental Implications

18. Risks of failure to meet statutory obligations as set out in paragraph 11. Health and safety implications for disabled staff and partners(for example) currently, before the works are completed

Contribution to Our Mission: *Safer Stronger Communities – Safe Effective Firefighters*

19. The Authority recognises that fire stations do not just exist for incident response but have a vital role in prevention and protection. Historically, few people would say that Fire Stations were inviting places with fire appliances barely visible behind closed doors. Merseyside Fire and Rescue Authority's vision is of true community hubs that provide a range of services working together to make Merseyside safer and stronger.

20. The stations very much belong to local communities and they need to be fully accessible to meet the needs of the community. Community Stations offer:
    - Inviting & welcoming community rooms and break out spaces.
    - Flexible facilities for our diverse community groups.
    - The community an increased sense of ownership.

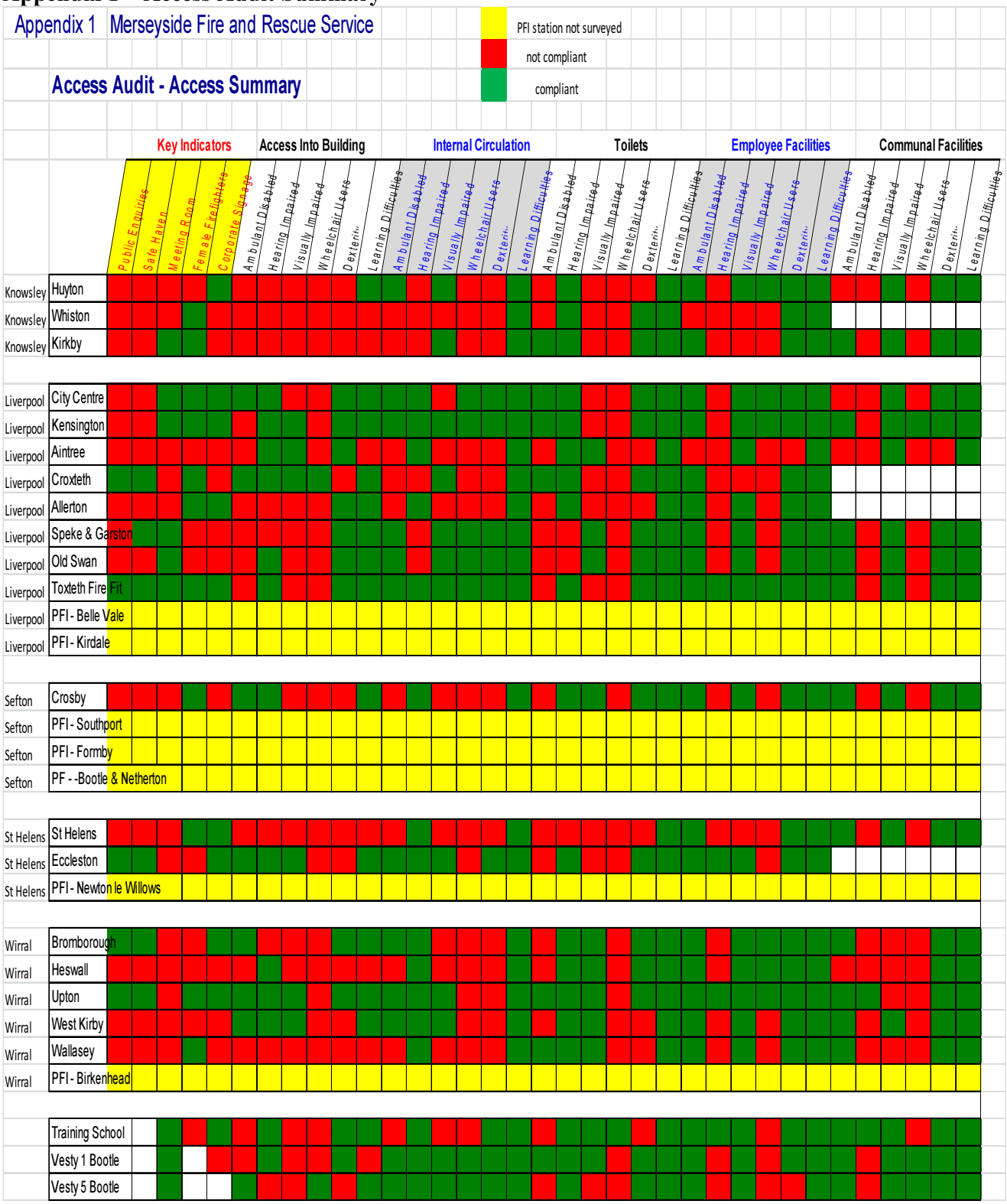
BACKGROUND PAPERS

CFO/111/11 If this report follows on from another, list the previous report(s)

GLOSSARY OF TERMS

This page is intentionally left blank

Appendix 1 – Access Audit Summary



This page is intentionally left blank

Appendix 2

Appendix 2 Merseyside Fire and Rescue Service

Access Audit - Cost Summary By Piroity & District

District	Station	Priority 1 DDA	Priority 2 Improvement	Priority 3 Best Practice	Priority 4 Operational	Female Firefighters	Total
Knowsley	Huyton	£18,300.00	£25,910.00	£615.00	£2,440.00	£3,200.00	£50,465.00
Knowsley	Whiston	£2,275.00	£1,915.00	£3,200.00	£6,215.00		£13,605.00
Knowsley	Kirkby	£11,515.00	£10,750.00	£1,520.00	£2,555.00		£26,340.00
	Knowsley Sub Total	£32,090.00	£38,575.00	£5,335.00	£11,210.00	£3,200.00	£90,410.00
Liverpool	City Centre	£7,300.00	£4,475.00	£6,015.00	£6,780.00		£24,570.00
liverpool	Kensington	£7,345.00	£8,875.00	£4,475.00	£3,700.00		£24,395.00
Liverpool	Aintree	£13,500.00	£9,765.00	£1,595.00	£1,700.00	£3,200.00	£29,760.00
Liverpool	Croxteth	£4,050.00	£7,505.00	£800.00	£17,135.00		£29,490.00
Liverpool	Allerton	£28,950.00	£6,975.00	£1,650.00	£2,340.00		£39,915.00
Liverpool	Speke & Garston	£10,645.00	£5,055.00	£5,045.00	£4,600.00	£3,200.00	£28,545.00
Liverpool	Old Swan	£20,405.00	£9,990.00	£3,045.00	£5,100.00	£3,200.00	£41,740.00
Liverpool	Toxteth Fire Fit	£29,700.00	£18,850.00	£11,550.00			£60,100.00
	Liverpool Sub Total	£121,895.00	£71,490.00	£34,175.00	£41,355.00	£9,600.00	£278,515.00
sefton	Crosby	£3,025.00	£26,420.00	£1,210.00	£1,340.00		£31,995.00
	Sefton Sub Total	£3,025.00	£26,420.00	£1,210.00	£1,340.00	£-	£31,995.00
st helens	St Helens	£50,950.00	£59,250.00	£14,000.00	£3,485.00		£127,685.00
st helens	Eccleston	£1,225.00	£13,425.00	£1,045.00	£4,295.00	£2,500.00	£22,490.00
	St Helens Sub Total	£52,175.00	£72,675.00	£15,045.00	£7,780.00	£2,500.00	£150,175.00
wirral	Bromborough	£15,275.00	£3,055.00	£3,050.00	£1,440.00	£1,500.00	£24,320.00
wirral	Heswall	£32,025.00	£6,650.00	£1,750.00	£875.00		£41,300.00
wirral	Upton	£10,475.00	£5,550.00	£720.00			£16,745.00
wirral	West Kirby	£13,325.00	£5,960.00	£9,700.00	£1,700.00	£6,200.00	£36,885.00
wirral	Wallasey	£29,150.00	£72,400.00	£11,500.00	£3,530.00		£116,580.00
	Wirral Sub Total	£100,250.00	£93,615.00	£26,720.00	£7,545.00	£7,700.00	£235,830.00
	Training School	£17,595.00	£22,905.00	£14,745.00		£5,700.00	£60,945.00
	Vesty 1 Bootle	£3,125.00	£13,690.00	£11,195.00	£1,875.00		£29,885.00
	Vesty 5 Bootle	£10,550.00	£7,140.00	£4,600.00			£22,290.00
	Total	£340,705.00	£346,510.00	£113,025.00	£71,105.00	£28,700.00	£900,045.00

This page is intentionally left blank

Appendix 3

Appendix 3 Cost Summary by Access Type

	Priority 1 DDA	Priority 2 Improvement	Priority 3 Best Practice	Priority 4 Operational	Total
Section 1 : External Circulation	£68,200.00	£31,010.00	£4,755.00	£4,650.00	£108,615.00
Section 2 : Building Entrance	£106,435.00	£33,790.00	£17,120.00	£14,715.00	£172,060.00
Section 3 : Reception	£6,700.00	£1,800.00	£300.00	£0.00	£8,800.00
Section 4 : Corridors / Circulation	£400.00	£135.00	£8,190.00	£475.00	£9,200.00
Section 5 : Internal Stairs	£30,825.00	£108,730.00	£20,725.00	£9,475.00	£169,755.00
Section 6 : Internal Ramps	£200.00	£4,400.00	£4,625.00	£3,750.00	£12,975.00
Section 7 : Internal Doors	£15,750.00	£67,495.00	£2,530.00	£20,460.00	£106,235.00
Section 8 : Wayfinding / Means of Escape	£2,900.00	£40,245.00	£18,650.00	£5,775.00	£67,570.00
Section 9 : Toilet Facilities	£35,440.00	£38,160.00	£12,805.00	£6,665.00	£93,070.00
Section 10 : Accessible Toilets	£56,855.00	£12,530.00	£5,825.00	£1,800.00	£77,010.00
Section 11 : Employee Facilities	£1,500.00	£2,400.00	£15,300.00	£2,940.00	£22,140.00
Section 12 : Communal Facilities	£15,500.00	£5,815.00	£2,200.00	£400.00	£23,915.00
Total	£340,705.00	£346,510.00	£113,025.00	£71,105.00	£871,345.00

This page is intentionally left blank

Appendix 4

Audit Cost Schedule - 2013

Issue 2

Ref	Item	Unit	Rate
1	External Tactile Paving	m2	£ 75.00
1	Alter kerbs	m	£ 60.00
1	Break up existing surfacing	m2	£ 5.00
1	Tarmac Pavement including base	m2	£ 45.00
1	Precast concrete paving	m2	£ 30.00
1	New kerbs	m	£ 35.00
1	Lighting Column	each	£ 2,500.00
1	Floodlight	each	£ 400.00
1	External Sign - 600 x 450	each	£ 250.00
1	External Sign - 300 x 200	each	£ 150.00
1	External Sign - small	each	£ 100.00
1	Disabled parking bay sign	each	£ 250.00
1	Mark out disabled bay - standalone	each	£ 400.00
1	Mark out disabled bay - other markings required	each	£ 250.00
1	Bench seat	each	£ 500.00
1	Access controls	each	£ 1,000.00
1	Bollard Light	each	£ 200.00
2	External Handrail - wall mounted	m	£ 90.00
2	External Handrail - surface mounted	m	£ 120.00
2	External ramp - low rise with steps (handrails extra)	m2	£ 500.00
2	External safety step cover	each	£ 75.00
2	Dwarf brick wall - including foundations	m	£ 150.00
2	Insitu concrete surfacing - including base	m2	£ 55.00
2	Additional hardcore to build up levels (150mm)	m2	£ 12.00
2	Re-position emergency telephone	each	£ 275.00
2	New aluminium door	each	£ 1,500.00
2	Widen external door	each	£ 800.00
2	Step Nosing	m	£ 40.00
2	Stainless Steel Pull Handles	each	£ 120.00

2	Intercom	each	£ 300.00
3	Call bell with indicator light	each	£ 100.00
4	Internal Fluorescent Light	each	£ 200.00
4	Lower Access Control	each	£ 100.00
5	Internal handrail - timber wall mounted	m	£ 90.00
5	Internal handrail - nylon coated wall mounted	m	£ 200.00
5	Internal handrail - nylon coated with infill panel	m	£ 330.00
5	Nosings	each	£ 25.00
7	Pull Handles / Push Plates	each	£ 50.00
7	Kick Plates	each	£ 30.00
7	Extended Vision Panel	each	£ 200.00
7	Internal widen single opening and fit new door	each	£ 900.00
7	Enlarge door opening	each	£ 525.00
7	Replace door	each	£ 400.00
7	New internal ironmongery	each	£ 120.00
7	Adjust door closer	each	£ 25.00
7	Replace closer	each	£ 150.00
8	Internal Sign - Medium	each	£ 100.00
8	Internal Sign - Small	each	£ 50.00
8	Install fire alarm call point	each	£ 150.00
8	Instal visual alarm	each	£ 100.00
8	Panic bar to external door	each	£ 150.00
8	Evac Chair	each	£ 800.00
8	Lower Call Point	each	£ 100.00
9	Basin taps	pair	£ 130.00
9	Wash-hand Basin	each	£ 600.00
9	Blending valves	each	£ 150.00
10	Grab rail	each	£ 90.00
10	fold down grab rail	each	£ 200.00
10	Back rest	each	£ 160.00
10	Emergency pullcord	each	£ 350.00

10	Coat Hook	each	£ 10.00
10	Extended Mirror	each	£ 300.00
11	Extend Light Switch	each	£ 90.00
11	Chair with arms	each	£ 75.00
11	Induction Loop	each	£ 700.00

This page is intentionally left blank

Appendix 5

Access Audit — Kirkby Community Fire Station

Address	Kirkby Community Fire Station	**te of Inspection**	29 April 2013
	Webster Drive		
	Kirkby. L32 8SJ	**Surveyor**	D Trowler BSc(Hons), MRICS, RMaPS, NRAC Consultant

Background Information

The building was opened in 1961 and is a two-storey building with the accommodation arranged in an L shape. The main accommodation block is located to the left-hand side and includes dormitory, toilets and office to the front with rest room and kitchen at the rear. Offices and female firefighters accommodation is located on the first floor.

The community rooms are located in a self-contained block to the right of the appliance bay. A gym is provided to the rear of the main building.

Use of Building

Members of the public may call at the Station to make enquiries.

The building has extensive community use including various community groups, local residents etc., all of whom use the community room. The gym is not used by the public.

Accessibility Summary

	Ambulant Disabled	Hearing Impaired	Visually Impaired	Wheelchair Users	Dexterity	Learning Difficulties
Access into Building						
Internal Circulation						
Toilets						
Employee Facilities						
Communal Facilities						

Key Indicators	
Public Enquiries	
Safe Haven	
Accessible Meeting Room	
Female Firefighter Facilities	
Corporate Signage	

Audit Strategy

Taking into account the use of the building and the needs of the various users we consider that the following need to be considered in developing an access strategy:

Public (P)
Access is required upto the main entrance and community facilities.
Visitors (V)
Visitors should be able to park, access the main entrance and be able to access office and meeting facilities. Suitable toilet facilities should also be made available.
Employees (E)
Employees require access to all areas of the building to fulfill their duties. The Act does not require adjustments to be made in anticipation of ever having a disabled employee.

Guidance Notes

Room References	Rooms are referenced with regard to the floor plans provided.	
Assessment	An assessment as to whether the premises complies with the requirements for each particular question	
	No = Unsatisfactory	
	Yes = Satisfactory	
Impairment Affect	A = Ambulant	
	H = Hearing	
	V = Visual	
	W = Wheelchair	
	D = Dexterity	
	L = Learning Difficulties	
Priority	Priority 1	Work to be required to ensure the services are accessible to the public. Improvements that will assist in complying with duties under the Disability Discrimination Act.
	Priority 2	Improvements to overcome problems with the existing site / building which would be beneficial to users with an impairment. Improvements beneficial to users but not required by Disability
	Priority 3	Recommendations considered Best Practice or to suit a potential future employee. Best Practice is considered to be work that is not required to fulfil a statutory duty but which would bring the item concerned up to modern standards with regard to access/facilities.
	Priority 4	Recommendations affecting accommodation only used by operational personnel.

Access Summary A detailed assessment of the existing arrangements is provided in the audit report but can be summarised as follows:

1. The paving leading to the main entrance is uneven. Steps are provided leading upto the entrance but the riser heights are unequal and no handrails are provided. There is no ramp.
2. The community rooms have a separate entrance from the rear yard. No access path is provided for pedestrians apart from the existing drive. There is a lack of signage to identify the community room.
3. A disabled parking space is provided in the yard however it is not located adjacent to the building.
4. There is no ramp to the entrance from the rear yard. This entrance would need to be used to access the toilets from the community rooms.
5. External doors are of suitable width but have raised thresholds and unsuitable handles.
6. The internal staircase is steep with narrow treads. The handrails are provided on one side only and difficult to grip.
7. Internal doors require upgrading to provide extended vision panels and replace ironmongery.
8. An accessible toilet is provided however it is incorrectly configured. There is a shower however the room is too small to accommodate this. The fittings are incorrectly positioned

Principle Recommend	1.	Relay paving leading to main entrance. Construct new access ramp and provide handrails to existing steps.
	2.	Relocate community room door to front of building and / or provide pedestrian footpath to side of drive.
	3.	Re-position disabled parking bay to outside community rooms.
	4.	Construct ramp to rear entrance and provide signage to indicate location of toilets.
	5.	Provide low profile thresholds to external doors and replace handles.
	6.	It is impractical to modify internal stairs and they are only used by operational staff. Handrails could be replaced.
	7.	Upgrade internal doors including providing extended vision panels and replacing ironmongery.
	8.	Remove shower from accessible toilet. Re-position fittings and support rails and change door to open outwards.

Cost Summary	Disability Discriminatic	£ 11,515.00
	Improvement	£ 10,750.00
	Best Practice	£ 1,520.00
	Operational Areas Onl	£ 2,555.00
	Female Firefighters Fa	£ -
	Total	£ 26,340.00

	Location	Description	Recommendation	Cost
Lockers	First Floor	Corridor outside study bedroom		£ -
Changing Facilities	First Floor	Separate study room		£ -
Toilets	First Floor	Ensuite to Study Room with shower, wc and basin.		£ -
Showers	First Floor	Within ensuite to Study Room		£ -
Sleeping Accommodation	First Floor	Separate study room		£ -
Washing & Toilet Facilities to Sleeping Accommodation	First Floor	Ensuite to Study Room with shower, wc and basin.		£ -
				£ -

Section 1 : External Circulation/Access

Kirkby Community Fire Station

			Person			Impairment Affected					
Ref	Question	Assessment	P	V	E	A	H	V	W	D	L	Comments	Recommendation	Priority	Cost
1.01	Is the building distinguishable from adjacent buildings?	Yes													
1.02	Is the building within convenient walking distance of public highway/	Yes													
1.03	Is there a suitable drop-off point for private cars close to the site entrance?	Yes													
1.04	Is the access route, within the boundary of the site even, level, free	Yes													
1.05	Is the access route, within the boundary of the site wide enough?	Yes										2400mm leading to front door			
1.06	Is the access route, within the boundary of the site surfaced with smooth, firm and slip-resistant	No	●	●	●	●		●	●			Paving slabs on approach to main entrance are slightly uneven with moss growing to	Relay uneven slabs and re-point joints to eliminate trip hazards.	2	£ 1,200.00
1.07	Is the access route, within the boundary of the site provided with aural, tactile and visual clues/warnings?	No	●	●				●	●	●		No defined route leading to Community Room entrance with pedestrians needing to use the access drive to reach the entrance which is located on the rear of the building.	Entrance should ideally be relocated to the front of the building with a corridor being formed to provide access to rooms. The other option would be to narrow the access drive by either marking out a pedestrian walkway or ideally constructing a footpath. The path should extend down to the public footpath.	1	£ 2,600.00
1.08	Is the access route, within the boundary of the site clearly signed or provided with landmarks to aid	No	●	●		●	●	●	●		●	No signage provided to indicate location of community room entrance which is at rear of	Provide directional signage adjacent to front entrance and along access route to side of	2	£ 300.00
1.09	Is the access route, within the boundary of the site adequately lit?	Yes													
1.10	Is the access route, within the boundary of the site free of hazards such as bollards, litter bins, manhole	Yes													
1.11	Is the access route, within the boundary of the site free of hazardous building features such as outward	No	●	●	●	●	●	●	●			Door to Community Room opens outwards over the pedestrian walkway parallel with the rear	If possible widen the path to allow clear access past the open door. Install guard rails on	2	£ 250.00
1.13	Are designated disabled parking bays provided?	Yes										Single bay is provided to right of entrance gates in rear yard.			
1.14	Is the disabled parking bay signposted from car park entrance?	No	●	●		●	●		●		●	No signage however proximity to gate means it is easy to find.			
1.15	Is the disabled parking bay clearly marked out?	No	●	●	●				●			Markings are beginning to deteriorate / fade. No post mounted sign.	Include for wall mounted sign to new space. (See 1.21)		
1.16	Is the disabled parking bay suitably sized?	No	●	●	●				●			4700mm x 2300mm compared with recommended size of 4800mm x 2400mm. No post mounted sign.	See 1.21		
1.17	Is the disabled parking bay suitably close to facilities served by car park?	Yes													
1.18	Is the disabled parking bay surfaced and in a good state of repair?	Yes													
1.19	Is the disabled parking bay adequately lit?	Yes													
1.20	Are sufficient number of disabled parking bays provided ?	Yes													
1.21	Is there a suitable access route from parking bay to building entrance?	No	●	●	●	●			●			Located on opposite side of drive which means users have to cross drive to reach community room and building. Visitors spaces are marked directly in front of the community room.	Re-locate space to in front of community room and provide 4800mm x 2400mm parking bay complete with 1200mm wide access zones.	2	£ 550.00
1.22	Is there suitable space for vehicles fitted with tail-lifts?	Yes										Rear yard			
1.24	Is external signage consistent and in accordance with current corporate	No										No signage to current standards. Old style community			
															£ 4,900.00

Section 2 : Building Entrance

Kirkby Community Fire Station

Ref	Question	Assessment	Person			Impairment Affected					Comments	Recommendation	Priority	Cost
			P	V	E	A	H	V	W	D	L				
2.01	Is the entrance to the building level?	No	●	●	●	○		○	○			Main Entrance - 3 no. steps			
2.01	Is the entrance to the building level?	No		●	●	○		○	○			Side Entrance - 1 no. step.			
2.01	Is the entrance to the building level?	Yes										Gym			
2.01	Is the entrance to the building level?	Yes										Community Room			
2.02	Are there less than two steps on the approach to the building entrance?	No	●	●	●	○		○	○			Main Entrance - 3 no. steps			
2.03	Are the steps provided with suitable handrails on both sides?	No	●	●	●	○		○				Main Entrance - No handrails provided.	Round profile handrails should be provided on either side and extend 300mm beyond top and bottom step. Handrails should be used to reduce width of steps to 1800mm to avoid need for a central handrail.	1	£ 350.00
2.04	Are the steps provided with visual and tactile warnings at top and bottom?	No	●	●	●			○				Main Entrance - No tactile warning provided.	As part of re-design to accommodate ramp ribbed tactile paving can be incorporated to landing and base of steps.		
2.05	Are the steps provided with treads of adequate length and of same length?	Yes													
2.06	Are the steps provided with non-slip finish to treads?	Yes													
2.07	Are the steps provided with uniform risers of suitable height and unlikely to trip users?	No	●	●	●	○						Main Entrance - Risers are 170mm / 170mm and 200mm. Bottom step is too high and unequal heights will cause problems.	Adjust level of paving on approach to reduce the riser height of the first step to 170mm. (See 1.06)		
2.08	Are the steps provided with readily identifiable nosings?	No	●	●	●			○				Main Entrance - No nosings.	Consider fitting slip resistant tread complete with coloured	2	£ 220.00
2.09	Are the steps provided with adequate lighting?	Yes													
2.10	Are the steps provided with landings of suitable size, including intermediate	Yes													
2.11	Is there a permanent entrance ramp?	No	●	●	●				○			Main Entrance - No ramp provided.	Sufficient space exists alongside steps to construct a ramp, complete with intermediate landing. Ramp should have handrails to both sides and kerbs to open sides. Length of ramp may be reduced through use of existing shallow gradients on approach to entrance.	1	£ 5,250.00
2.11	Is there a permanent entrance ramp?	No	●	●	●				○			Side Entrance - No ramp provided.	This would be the primary entrance from the rear yard and would be used by community room users to access the toilets and therefore requires ramped access. Ramp should have handrails to both sides and kerbs to open sides.	1	£ 1,100.00
2.12	If no ramp is provided, would a portable ramp be a suitable option?	No	●	●	●				○			Main Entrance			
2.20	Is the emergency telephone accessible to all users ?	No	●			○			○			1140mm high but located to side of entrance door and only accessible by steps which are unsuitable.	Relocate to wall at base of steps. Mounting height to be 1000mm.	1	£ 275.00
2.21	Where access is only by steps is there a bell or intercom at the bottom of the steps at a suitable height and with correct signage?	No	●	●	●				○			Main Entrance - Bell is at top of steps. No bell to side entrance.	See 2.11		
2.22	Is the entrance door easy to find and clearly distinguishable from the	Yes										Main Entrance			
2.22	Is the entrance door easy to find and clearly distinguishable from the	No	●			○	○	○	○		○	Community Room - No signage to identify.	Provide sign adjacent to door.	2	£ 150.00
2.23	Is a canopy provided over the entrance or are the entrance doors	No	●	●	●	○			○			Main Entrance	Not considered necessary		
2.24	Is the door approach level for a minimum of 1200mm clear of any door	No	●	●	●	○			○			Main Entrance - 175mm step at door threshold.	See 2.11		
2.24	Is the door approach level for a minimum of 1200mm clear of any door	No		●	●	○			○			Side Entrance - 450mm going and 150mm step at door	See 2.11		
2.24	Is the door approach level for a minimum of 1200mm clear of any door	Yes										Community Room			
2.25	Is the entrance door opening wide enough for all users?	Yes										Main and Side Entrances			

2.25	Is the entrance door opening wide enough for all users?	Yes	Gym				
2.25	Is the entrance door opening wide enough for all users?	Yes	Community Room				
2.26	Does the entrance door have a level or flush threshold?	Yes	Main Entrance				
2.26	Does the entrance door have a level or flush threshold?	No	Side Entrance - 30mm high threshold.	Replace with low profile threshold	2	£	75.00
2.26	Does the entrance door have a level or flush threshold?	No	Gym - 40mm high threshold.	Replace with low profile threshold	4	£	75.00
2.26	Does the entrance door have a level or flush threshold?	No	Community Room - 25mm high threshold.	Replace with low profile threshold	2	£	75.00
2.27	Is the entrance door glazing in safety glass?	Yes					
2.28	Are glass doors fitted with distinguishable warning strips?	Yes					
2.29	Is the entrance door easy to open with suitable handles at correct height?	No	Main Entrance - Door handle profile is difficult to grip. Excessive force required to open door. Thumb turns provided at 1160mm and 1520mm.	Replace handles with round profile nylon coated handles. Adjust door closer. Consider removal of top thumb turn.	2	£	300.00
2.29	Is the entrance door easy to open with suitable handles at correct height?	No	Side Entrance - Door handle profile is difficult to grip. Thumb turns provided at 1180mm and 1480mm.	Replace handles with round profile nylon coated handles. Adjust door closer. Consider removal of top thumb turn.	2	£	300.00
2.29	Is the entrance door easy to open with suitable handles at correct height?	No	Kitchen Entrance - Door handle profile is difficult to grip. Thumb turns provided at 1180mm and 1480mm.	Replace handles with round profile nylon coated handles. Consider removal of top thumb turn.	4	£	240.00
2.29	Is the entrance door easy to open with suitable handles at correct height?	No	Gym - Door handle profile is difficult to grip.	Replace handles with round profile nylon coated handles.	4	£	240.00
2.29	Is the entrance door easy to open with suitable handles at correct height?	No	Community Room - Door handle profile is difficult to grip.	Replace handles with round profile nylon coated handles.	2	£	240.00
2.30	Does the colour of handles contrast with door?	Yes	Main Entrance				
2.31	Is the entrance door fitted with delayed or slow action door closers?	Yes	Main Entrance				
2.32	Is the entrance door fitted with protective strip at the bottom of the	Yes	Main Entrance				
2.33	Can people each side of door, either standing or seated, see each other	Yes	Main Entrance & Community Room				
2.33	Can people each side of door, either standing or seated, see each other	No	Side Entrance - Vision panel is only provided to upper half of	Replace lower infill panel with glazing.	2	£	100.00
2.34	If an access control system is used for access, is the system suitable for use by and within reach of people with sensory or mobility impairments?	No	Main Entrance - Door bell to right of door is 1500mm high.	Bell should be lowered to 1200mm and replaced with one that includes a visual indicator.	1	£	100.00
2.37	Does the lobby provide a clear view in from the outside?	No	Mirrored reflective film on the front entrance door restricts vision from people waiting outside to see approaching persons inside the station.	Consider replacement with clear glass if film cannot be removed.	3	£	200.00
2.38	Is the inner entrance door opening wide enough for all users?	Yes					
2.39	Is the inner entrance door easy to open with suitable handles at correct	No	Door is of suitable width however handles may be	Replace with round profile ironmongery.	2	£	120.00
2.40	Does the colour of handles to the inner door contrast with door?	Yes					
2.41	Is the inner entrance door fitted with delayed or slow action door closers?	Yes					
2.42	Is the inner entrance door fitted with protective strip at the bottom of the	No	No kick plate.	Provide kick plate to push side of door.	3	£	30.00
2.43	Can people each side of inner door, either standing or seated, see each	Yes					
2.44	Is the lobby of adequate size to allow wheelchair users to move clear of one door before approaching and opening	Yes					
2.45	Is there a firm and flush entrance mat of adequate size?	No	Coir matting to front and side entrances.	Replace with modern barrier matting.	3	£	150.00
2.46	Is transitional lighting provided within lobby?	Yes					
						£	9,590.00

Section 4 : Corridors / Circulation

Kirkby Community Fire Station

Ref	Question	Assessme	Person	Impairment Affected						Comments	Recommendation	Priority	Cost
			P	V	E	A	H	V	W	D	L				
4.01	Are corridors wide enough for a wheelchair user to manoeuvre and for other people to pass?	Yes										Main corridors are at least 1700mm wide. Two short corridors are only 1220mm wide and these provide access to Toilets / Night Room and Office / Appliance Bay. There is also a short section of corridor to the rear of the kitchen providing access to the toilet and external door. Clear width is 1150mm.			
4.02	Are corridors free from obstructions to wheelchair users and from hazards to	Yes													
4.03	Is there adequate turning space for wheelchair users?	Yes													
4.04	Are floor surfaces suitable for passage of wheelchairs?	Yes													
4.05	Are junctions between different floor surfaces correctly detailed?	Yes													
4.06	Are floor surfaces slip-resistant?	Yes													
4.07	Are there no bright or boldly patterned floor coverings?	Yes													
4.08	Do walls, floors and doors contrast in colour and have surfaces that are non-	Yes													
4.09	Is adequate well-positioned lighting provided? Is natural and artificial lighting designed to avoid glare and	Yes													
4.11	Are internal lobbies of adequate size to allow wheelchair users to clear one door before approaching the second?	Yes													
															£ -

Section 5 : Internal Stairs / Lift

Kirkby Community Fire Station

Ref	Question	Assessme	Person	Impairment Affected						Comments	Recommendation	Priority	Cost
			P	V	E	A	H	V	W	D	L				
5.01	Are stair locations adequately signed with clear visual information at each	Yes										Located on main corridor in close proximity to entrances.			
5.02	Are visual and tactile warnings provided at the top and bottom of each flight?	No	●	●			●					No warnings provided - not considered necessary given configuration of stairs in two storey building			
5.03	Are suitable continuous, easy to grip, colour contrasting handrails provided to each side?	No	●	●		●				●		Handrail is provided on one side only and does not extend for the full length of the staircase. Profile is difficult to grip. At the bottom the open side of the stairs is protected by three vertical metal bars, with no handrail.	Provide round profile timber or coated handrails, maximum 50mm diameter to both sides. Where practical extend 300mm beyond top and bottom and ensure rails are continuous around landings.	2	£ 4,000.00
5.04	Do handrails extend 300 mm beyond top and bottom steps?	No	●	●		●		●				No projection to base of stairs.	See 5.04		
5.05	Is the staircase wide enough, with treads of uniform length and suitable width?	No	●	●		●						960mm clear width which is slightly narrower than recommended. 230mm going compared with minimum of 250mm.	Impractical to modify without replacement of the staircase. Accommodation is under utliised with access only being required by operational staff.		
5.06	Are all risers of the same height, shallow enough with no open or ribbed	No	●	●		●						190mm riser compared with maximum of 170mm.	See 5.05		
5.07	Are all nosings easily identifiable?	Yes													
5.08	Are landings of suitable size provided at intermediate levels in long flights?	Yes													
5.09	Are stairs free from obstructions to users and from hazards to people with	No	●	●		●		●				Desk stored at top of stairs restricts access.	Remove desk.		
5.10	Is adequate well-positioned lighting provided?	Yes													
5.11	Is a passenger lift available?	No	●	●		●				●		No lift to small first floor section of building.	Impractical to install a lift. It would be more cost effective to relocate the offices to the ground floor if access is required by a wheelchair user.		
															£ 4,000.00

Section 7 : Internal Doors

Kirkby Community Fire Station

Ref	Question	Assessment	Person Affected: P	V	E	A	H	V	W	D	L	Comments	Recommendation	Priority	Cost
7.01	Are doors absolutely necessary for safety or functional reasons?	Yes													
7.02	Are they distinguishable from their surrounds? Are glass doors clearly visible when closed?	No	●	●			●					Poor colour contrast to Kitchen Toilet door and small meeting room door to Community Rooms.	Re-decorate doors or frames in a contrasting colour when due for re-decoration.		
7.03	Do doors have bottom edge protection?	No	●	●	●			●				General lack of kick plates to ground floor.	Provide kick plates to 9 no. doors.	3	£ 270.00
7.04	Can people each side of the door, either standing or seated in a wheelchair, see each other and be	No	●	●	●		●					Where vision panels are provided they are only to upper section of door.	Provide vision panel from 500mm to 1500mm to 10 no. doors.	2	£ 2,000.00
7.05	Are clear opening widths sufficient for a wheelchair user?	Yes										Where wheelchair accessible			
7.06	Is there sufficient space alongside the leading edge for a wheelchair user or someone with limited mobility to reach the door control while clear of its	No	●	●				●				Restricted clearance to office door.	Modification not considered necessary as visitors will be accompanied.		
7.07	Are door controls at a height suitable for both standing and seated users?	No		●				●				High level locks to 2 no. doors. Only used by operational staff.			
7.08	Are controls clearly distinguishable from the door itself and easy to grasp?	No	●	●					●			Door controls to 3 No. doors are unsuitable.	Replace ironmongery to 3 no. doors.	4	£ 360.00
7.09	Are doors easy to open with door closers of an appropriate type requiring minimum opening pressure?	Yes													
															£ 2,630.00

Section 8 : Wayfinding/Means of Escape

Kirkby Community Fire Station

Ref	Question	Assessment	Person Affected: P	V	E	A	H	V	W	D	L	Comments	Recommendation	Priority	Cost
8.01	Are direction and information signs clearly visible from both a standing and seated position?	No	●	●		●	●	●	●		●	Minimal signage provided.	Not considered necessary as public access is restricted to Community Room and visitors are escorted.		
8.02	Are signs tactile?	No	●	●	●			●				Only tactile sign is to 1 no. toilet door.	Tacticle signs could be provided to Community Room	2	£ 120.00
8.04	Is the overall layout of the building reasonably clear and logical?	Yes													
8.08	Are fire alarm points capable of being operated by a wheelchair user?	Yes										Community Room			
8.09	Is the audible alarm system supplemented by a visual system?	No	●	●		●						Sounder only	Visual alarm could be installed in the Community Room and	3	£ 100.00
8.10	Are ground floor exit routes as accessible to all, including wheelchair users, as entrance routes?	No		●	●		●	●	●			Single step to all exit doors.	See Section 2 for improvements to Main and Side Entrances. Kitchen corridor exit door could have a level landing constructed externally. Only	4	£ 300.00
8.12	Are the exits clearly signed?	No	●	●	●	●	●	●	●		●	Rear ground floor lacks fire exit signage.			
8.13	Can doors be opened by a disabled person?	No	●	●	●			●	●			External doors have thumb turns which are too high and	Install panic latch to exit door. Remove upper thumb turns to	2	£ 250.00
8.14	If people with disabilities cannot completely evacuate the building can	Yes													
															£ 770.00

Section 9 : Toilet Facilities

Kirkby Community Fire Station

Ref	Question	Assessment	Person P	Person V	Person E	Impairment Affected A	Impairment Affected H	Impairment Affected V	Impairment Affected W	Impairment Affected D	Impairment Affected L	Comments	Recommendation	Priority	Cost
9.01	If a lobby is provided, is it of sufficient size to allow for easy access?	No		●		●						First Floor Toilet - 800mm gap between screen and wall.			
9.02	Are lobby doors light enough to open easily?	Yes													
9.03	Do all toilet areas have slip-resistant floors?	No		●		●						First Floor Toilet does not have a slip resistant floor	Replace with safety flooring when toilets refurbished.		
9.04	Are fittings readily distinguishable from the background?	No		●			●					First Floor Toilet - Modesty screen is same colour as walls.	Decorate doors or frames in a contrasting colour.	4	£ 50.00
9.05	Are compartment door controls/locks easily gripped and operated?	No		●					●			Kitchen Toilet has simple barrel bolt.	Replace with bathroom privacy lock with extended lever thumb turn and coloured indicator bolt.	4	£ 40.00
9.06	Are fittings such as flushes to the toilet and light switches usable by people	Yes													
9.07	Is there sufficient space for ambulant disabled people to manoeuvre?	Yes													
9.08	Can ambulant disabled people raise and lower themselves in standard	No	●	●	●	●						No support rails provided	Accessible Toilet is provided.		
9.09	If the door opens inwards can it be opened outwards or removed easily in	No			●	●						First floor toilet has standard inward opening door.	Room is of sufficient size to allow a cubicle to be installed.		
9.10	Is the travel distance to a suitable WC no greater than that for able-bodied	Yes										No toilets are provided within the Community Rooms section.			
9.11	Is provision made for wheelchair users?	Yes										Ground floor of main building.			
9.12	Are taps appropriate for use by a person with limited dexterity, grip or	Yes													
9.13	Is the water temperature appropriate?	No	●	●	●	●				●	●	Hot water in all toilets.	Install blending valves	3	£ 450.00
															£ 540.00

Section 10 : Accessible Toilets

Kirkby Community Fire Station

Ref	Question	Assessment	Person P	Person V	Person E	Impairment Affected A	Impairment Affected H	Impairment Affected V	Impairment Affected W	Impairment Affected D	Impairment Affected L	Comments	Recommendation	Priority	Cost
10.01	Is the WC approachable by a wheelchair user - i.e. free of steps, corridor obstructions, narrow doors etc?	No	●						●			Community Room users need to exit building and use side entrance door into main building. This door has a step and is not currently wheelchair accessible.	See Section 2 for improvements to door to provide ramp.		
10.02	Is the travel distance to the accessible toilet satisfactory?	Yes													
10.03	Is the location clearly signed?	No	●	●		●			●			No signage in corridor apart from sign on door itself.	Provide signage in Community Rooms lobby to indicate location of toilets. Provide directional signage in lobby area from side entrance.	2	£ 100.00
10.04	Is there sufficient space outside the toilet compartment for manoeuvre and	Yes													
10.05	Are door controls, locks and light switch easily reached and operated?	No	●	●	●				●			Door opens inwards and has a standard thumb turn lock. Shower obstructs access to	Door needs to be changed to open outwards. Lighting should be changed to sensor operated	1	£ 250.00
10.06	Is the compartment large enough to allow manoeuvring into position for frontal, lateral, angled and backward transfer unassisted and with assistance?	Yes										2500mm x 1500mm			
10.07	Is the manoeuvring area free from obstructions e.g.. boxed-in pipes or	No	●	●	●				●			Shower adjacent to door.	Room is too small to incorporate a shower and this therefore	1	£ 500.00
10.08	Is the WC layout correctly handed for a left or right-sided approach.	No	●	●	●				●			WC Suite is on side wall to rear left-hand wall with the basin adjacent on the rear wall.	WC suite needs to be moved to the rear wall in left-hand corner and basin to side wall adjacent.	1	£ 550.00
10.09	Are fittings arranged to facilitate easy manoeuvre?	No	●	●	●				●			No coat hooks or extended mirror.	Provide coat hooks at 1050mm and 1400mm high. Provide mirror from 600mm to 160mm.	3	£ 320.00
10.10	Do walls, floor and door surfaces contrast in colour and have surfaces	Yes													
10.11	Is there a suitable emergency alarm call system ?	No	●	●	●	●			●			No emergency call system	Install new emergency alarm system complete with pull cord and overdoor light. Reset switch to be adjacent to wc.	1	£ 350.00
10.12	Are hand washing and drying facilities within easy reach of someone seated	No	●	●	●				●			Basin is fixed too far forward of wc pan at 260mm.	Re-position as part of toilet alterations and 140-160mm		
10.13	Are taps appropriate for use by a person with limited dexterity, grip or	Yes													
10.14	Is the water temperature appropriate?	Yes													
10.15	Are suitably designed grab rails fitted in all positions necessary to assist manoeuvring?	No	●	●	●	●			●			Horizontal rail is fixed too far forward of rear corner and too high. No rail to door.	All rails require re-positioning as part of alterations to layout. Provide additional horizontal rail to door.	1	£ 190.00
10.16	Is the flush handle correctly positioned?	Yes													
															£ 2,260.00

Section 11 : Employee Facilities

Kirkby Community Fire Station

Ref	Question	Assessment	Person Impairment Affected							Comments	Recommendation	Priority	Cost
			P	V	E	A	H	V	W				
11.01	Are suitable designated disabled parking bays provided for staff (state	Yes								1 no. space in yard. (See Section 1)			
11.02	Is external communication possible by minicom (text-phone) as well as a	No			●	●				None provided	Provide if needed to suit a specific need		
11.03	Are induction loops fitted in conference/ meeting rooms?	No			●	●				None Provided. Not considered necessary.	Provide if needed to suit a specific need		
11.04	Are suitable staff welfare facilities available on an accessible floor?	Yes											
11.05	Are tea point or kitchen facilities set out appropriately for all users?	Yes								Kitchen has stainless steel units / benches at standard height with no clear space beneath for wheelchair users. Only used by operational staff.			
11.05	Are tea point or kitchen facilities set out appropriately for all users?	No			●	●		●		Small kitchenette is provided to end of first floor corridor. 470mm clear width between table and fridge.	If kitchen is to be provided on the first floor it would be better to replace the toilets with a new kitchen.		
11.06	Are staff facilities suitably located with regard to the location of access points and work areas ?	No			●	●			●	Kit Room is an external portakabin. 280mm step at entrance. Door is of suitable width but handle is unsuitable profile.	Provide new steps incorporating 2 no. risers and level landing to top. Provide handrails to both side and around landing. Replace door furniture	4	£ 1,250.00
11.07	Is the room free from hazards to people with impaired sight ?	No			●		●	●		Gym equipment is similar tone to flooring and some items have projecting feet which could be a potential hazard. Clear space between equipment is very limited and creating a hazard particularly where there are moving parts.	Ideally the number of machines should be reduced and all the machines arranged to provide a clear access route. Alternative floor colour should be used when due for replacement.		
11.08	Is the room laid out in a such a way as to allow free access by wheelchair users ?	No			●		●	●		Very restricted circulation space in the small single bedroom off the main dormitory.	Two other larger rooms are available and only used by operational personnel.		
11.08	Is the room laid out in a such a way as to allow free access by wheelchair users ?	No			●		●	●		Office to Rear Corridor - limited circulation due to amount of furniture. 430mm clearance	Re-arrange furniture to improve circulation space.		
11.08	Is the room laid out in a such a way as to allow free access by wheelchair users ?	No			●		●	●		Limited clearance in one of the study rooms - 530mm clear width between door and bed.	Two other larger rooms are available and only used by operational personnel.		
11.09	Are light switches/sockets at suitable height for employees with restricted	No			●			●		1400mm generally. Pull cord in Gym is 1660mm high.	Lower switches or install automatic lighting controls if		
11.10	Are floor surfaces suitable for passage of wheelchair users with correctly detailed joints between	Yes											
11.11	Do walls, floor and door surfaces contrast in colour and have surfaces	Yes											
11.12	Are lockers / storage facilities accessible to all users ?	Yes											
11.13	Is suitable seating / tables provided for wheelchair users and the ambulant	Yes											
													£ 1,250.00

Section 12 : Communal Facilities

Kirkby Community Fire Station

Ref	Question	Assessment	Person Impairment Affected							Comments	Recommendation	Priority	Cost
			P	V	E	A	H	V	W				
12.01	Are communal facilities accessible to all users ?	Yes											
12.02	Are conference / meeting rooms accessible to all users ?	Yes											
12.03	Are induction loops fitted in conference/ meeting rooms?	No		●	●	●				None Provided. Not considered necessary.			
12.04	Is the room free from hazards to people with impaired sight ?	Yes											
12.05	Is the room laid out in a such a way as to allow free access by wheelchair users ?	No	●					●		Community Room Lobby - small kitchen provided adjacent to door. Standard unit height with no clear space for wheelchair user.	If kitchen facility is to be provided consider a lowered base unit 850mm high with clear space beneath to allow for use by a wheelchair user.	2	£ 400.00
12.06	Are light switches/sockets at suitable height for users with restricted	Yes											
12.07	Are floor surfaces suitable for passage of wheelchair users with correctly detailed joints between different surfaces?	Yes											
12.08	Do walls, floor and door surfaces contrast in colour and have surfaces	Yes											
12.09	Is suitable seating / tables provided for wheelchair users and the ambulant	Yes											
													£ 400.00

Cost Summary

Kirkby Community Fire Station

	Priority 1 DDA	Priority 2 Improvement	Priority 3 Best Practice	Priority 4 Operational	Total
Section 1 : External Circulation	£ 2,600.00	£ 2,300.00			£ 4,900.00
Section 2 : Building Entrance	£ 7,075.00	£ 1,580.00	£ 380.00	£ 555.00	£ 9,590.00
Section 3 : Reception					£ -
Section 4 : Corridors / Circulation					£ -
Section 5 : Internal Stairs		£ 4,000.00			£ 4,000.00
Section 6 : Internal Ramps					£ -
Section 7 : Internal Doors		£ 2,000.00	£ 270.00	£ 360.00	£ 2,630.00
Section 8 : Wayfinding / Means of Escape		£ 370.00	£ 100.00	£ 300.00	£ 770.00
Section 9 : Toilet Facilities			£ 450.00	£ 90.00	£ 540.00
Section 10 : Accessible Toilets	£ 1,840.00	£ 100.00	£ 320.00		£ 2,260.00
Section 11 : Employee Facilities				£ 1,250.00	£ 1,250.00
Section 12 : Communal Facilities		£ 400.00			£ 400.00
Total Cost	£ 11,515.00	£ 10,750.00	£ 1,520.00	£ 2,555.00	£ 26,340.00

7.03 Bottom Edge Protection	7.04 Vision Panels	7.05 Opening Width	7.06 Leading Edge	7.07 Control Height	7.08 Control Type	7.09 Door Closers
Watch Room	Watch Room		Office G18	Appliance Bay	Dormitory Corridor	
Dormitory Corridor	Dormitory Corridor			Dormitory Corridor	BA Room	
Cross Corridor	Cross Corridor				Community Rooms x 1	
Training Room	Training Room					
Mess Room x 2	Mess Room x 2					
Kitchen x 2	Kitchen x 2					
Community Rooms x 1	Community Rooms x 2					

This page is intentionally left blank

Appendix 6
Revised schedule of Priority 1 Access works and Female Firefighter Faculties

Table 1 Works required for Female Firefighters Facilities		
District	station	Costs
Knowsley	Huyton	£3,200.00
Liverpool	Aintree	£3,200.00
Liverpool	Speke & Garston	£3,200.00
Liverpool	Old Swan	£3,200.00
Liverpool	Training school	£5,700.00
St Helens	Eccleston	£2,500.00
Wirral	Bromborugh	£1,500.00
Wirral	West Kirby	£6,200.00
Liverpool	Training school	£5,700.00
	Total	£34,400.00

Table 2 Works required to comply with Equality Act		
District	station	cost
Knowsley	Kirkby	£11,515.00
Liverpool	City Centre	£7,300.00
Liverpool	Kensington	£7,345.00
Liverpool	Croxteth	£4,050.00
Liverpool	speke & Garston	£10,645.00
Liverpool	Old Swan	£20,405.00
Liverpool	Toxteth	£29,700.00
Liverpool	Training school	£17,595.00
Liverpool	Vesty 1	£3,125.00
Liverpool	Vesty 5	£10,550.00
Sefton	Crosby	£3,025.00
Wirral	Bromborugh	£15,275.00
Wirral	Heswall	£32,025.00
Wirral	Wallasey	£29,150.00
Knowsley	Huyton	£18,300.00
Knowsley	whiston	£2,275.00
Liverpool	Aintree	£13,500.00
Liverpool	Allerton	£28,950.00
St Helens	St Helens	£50,950.00
St Helens	Eccleston	£1,225.00
Wirral	Upton	£10,475.00
Wirral	West Kirby	£13,325.00

Total	£340,705.00

Table 3 Phase 1		
District	station	
Knowsley	Kirkby	£11,515.00
Liverpool	Croxteth	£4,050.00
Liverpool	Training school	£17,595.00
Liverpool	Toxteth	£29,700.00
Sefton	Crosby	£3,025.00
Wirral	Wallasey	£29,150.00
	Total	£95,035.00

Table 4 -Phase 2		
District	station	
Liverpool	City Centre	£7,300.00
Liverpool	Kensington	£7,345.00
Liverpool	Old Swan	£20,405.00
Liverpool	Speke & Garston	£10,645.00
Liverpool	Vesty 1	£3,125.00
Liverpool	Vesty 5	£10,550.00
Wirral	Heswall	£32,025.00
Liverpool	Aintree	£13,500.00
Liverpool	Allerton	£28,950.00
	Total	£133,845.00

Table 5- Phase 3		
District	station	
Knowsley	Huyton	£18,300.00
Knowsley	whiston	£2,275.00
St Helens	St Helens	£50,950.00
St Helens	Eccleston	£1,225.00
Wirral	Upton	£10,475.00
Wirral	West Kirby	£13,325.00
	Total	£96,550.00

MERSEYSIDE FIRE AND RESCUE AUTHORITY			
MEETING OF THE:	**POLICY AND RESOURCES COMMITTEE**		
DATE:	**1 APRIL 2014**	**REPORT NO:**	**CFO/012/14**
PRESENTING OFFICER	**DEPUTY CHIEF FIRE OFFICER**		
RESPONSIBLE OFFICER:	**DEB APPLETON**	**REPORT AUTHOR:**	**DEB APPLETON**
OFFICERS CONSULTED:	**PROTECTIVE SECURITY GROUP**		
TITLE OF REPORT:	**PROTECTIVE SECURITY POLICY AND RELATED SERVICE INSTRUCTIONS**		

APPENDICES:	**APPENDIX A:**	**DRAFT PROTECTIVE SECURITY POLICY**
	APPENDIX B:	**DRAFT PROTECTIVE MARKING SERVICE INSTRUCTION**
	APPENDIX C:	**DRAFT PERSONNEL SECURITY SERVICE INSTRUCTION**
	APPENDIX D:	**EQUALITY IMPACT ASSESSMENT**

Purpose of Report

1. To request that Members consider and approve the attached Policy and Service Instructions that have been developed to enable the Authority to implement the requirements of the Government's Protective Security Strategy.

Recommendation

2. That Members approve the Protective Security Policy, Protective Marking Service Instruction and Personnel Security Service Instruction attached as appendices A, B and C respectively. All of these documents have been through the Authority's consultation process with some minor changes being made as a result.

Introduction and Background

3. Protective Security is the term used to describe the actions/policies required to meet the threats to an organisation and to protect its assets from compromise. Protective Security is important when considering the political climate and the technology that poses threats and risks to the Fire and Rescue Authority. Effective security is important in maintaining the confidence of the public, staff, stakeholders and partner agencies in efficient, effective and safe service delivery. Protective Security is a holistic process that covers three related aspects of security; information (documents/data systems), personnel (staff/customers) and physical (buildings/estates/property).

4. The Authority's aim is to achieve compliance, as far as practicable, with the relevant aspects of HMG Security Policy Framework, and as detailed within the DCLG Fire & Rescue Protective Security Strategy. There are close links with Information Security and Governance, resilience, ICT security and building management. A working group with representatives from all related areas has been set up to implement the requirements of the Fire and Rescue Service Protective Security Strategy and Protective Security related roles, as set out in the FRS Strategy, have been allocated to staff as outlined below:

   Protective Security Lead - Deputy Chief Fire Officer
   Service Security Officer (SSO) – Group Manager – Operational Preparedness
   Information Technology Security Officer (ITSO) - ICT Applications Manager
   Senior Information Risk Owner (SIRO) - Director of Strategy and Performance
   Information Asset Owners (IAO) – at least one employee has been allocated this role in each department

5. The working group has produced the draft Protective Security Policy (Appendix A) which sets out how MFRA intends to comply with these requirements in general terms. In addition two new draft Service Instructions (attached at Appendices B and C) set out in more detail how new processes will be implemented to deliver against two important aspects of Protective Security; protective marking of information assets and personnel related security. Information Asset Owners are currently being given guidance as to their role and other Service Instructions will be developed as required to either enhance existing arrangements or introduce any new processes that are identified by the working group.

Protective Marking

6. Protective marking of information assets is an important element of Protective Security as it allows for a co-ordinated way of implementing an appropriate level of protective controls against the likely threat to sensitive information. The current scheme used is the Government Protective Marking Scheme, but this will change to the Government Security Classifications (GSC) on 2nd April 2014. As a result, it is proposed that MFRA starts to mark its information assets using the new GSC system and this is reflected in the Service Instruction. As this is a major piece of work the Authority will take a risk based approach with the Protective Security lead officers working with the Information Asset Owners to identify when information assets should be marked.

Personnel Security

7. The purpose of Personnel Security is to provide a level of assurance as to the trustworthiness, integrity and reliability of Service employees, volunteers and contractors. The draft Service Instruction sets out that as a minimum requirement all staff will be subject to recruitment controls known as the Baseline Personnel Security Standard. This consists of the verification of unspent criminal records. This will however be phased in, beginning with new recruits. Information Asset Owners will then work with the Protective Security

lead officers to identify in which order departments or staff require the checks to be carried out according to the Protective Security risk associated with each department. The other enhanced vetting processes referred to within this Service Instruction apply to a very small number of senior staff and are already in place.

Equality and Diversity Implications

8. An Equality Impact Assessment has been carried out and the initial findings are attached. The EIA will be reviewed and updated as the implementation of Protective Security progresses.

Staff Implications

9. There are implications associated with the implementation of the Baseline Personnel Security Standard as this involves the use of a new security check. However, enhancing Personnel Security is essential for compliance with the requirements of the Protective Security Strategy and these implications are currently being considered by People and Organisational Development.

Legal Implications

10. The Authority is a Category 1 responder under the Civil Contingencies Act 2004 and as such has a duty to assess, plan and advise in relation to certain emergencies. The Authority has a duty to keep information it holds in relation to this duty secure and this policy seeks to ensure the security of such information.

11. The Authority has duties under the Data Protection Act 1998 to keep personal information secure and should take steps to ensure such data is protected against loss or theft. This policy is one of a number of measures in place to protect personal information ensuring compliance with these statutory obligations.

Financial Implications & Value for Money

12. There are financial implications associated with the implementation of the Baseline Personnel Security Standard across the Service. Initially this will be limited to new recruits. This will however extend to all other staff through the risk based approach, which will take some time. Each check costs £25 and the current budget is £1,500 which limits the rate at which the process can be implemented.

Risk Management, Health & Safety, and Environmental Implications

13. Protective Security is a strategy to reduce risk, so all parts of the Strategy will help to improve Merseyside Fire and Rescue Authority's resilience.

14. There are some risk implications in relation to storing RESTRICTED and potentially OFFICIAL-SENSITIVE information on the MFRA network, but it is considered that it is operationally important to do so and systems will be put in place to ensure that information is kept as securely as possible.

15. There are no health, safety or environmental implications.

Contribution to Our Mission: *Safer Stronger Communities – Safe Effective Firefighters*

16. Implementation of the Protective Security Strategy will help improve security within all areas of Merseyside Fire and Rescue Authority.

BACKGROUND PAPERS

GLOSSARY OF TERMS

Merseyside FIRE & RESCUE SERVICE
"An Excellent Authority"

Policy STRPOL14

APPENDIX A

Document Control

Description and Purpose

The Purpose of this Policy is to outline the Authority's approach to Protective Security

Active date	Review date	Author	Editor	Publisher
		Deb Appleton	Deb Appleton	

Permanent	X	Temporary		If temporary, review date must be 3 months or less.

Amendment History

Version	Date	Reasons for Change	Amended by

Risk Assessment (if applicable)

Date Completed	Review Date	Assessed by	Document location	Verified by(H&S)

Equalities Impact Assessment

Initial	Full	Date	Reviewed by	Document location

Civil Contingencies Impact Assessment (if applicable)

Date	Assessed by	Document location

Related Documents

Doc. Type	Ref. No.	Title	Document location
Service Instruction	SI0816	PROTECTIVE MARKING - GOVERNMENT SECURITY CLASSIFICATIONS AND GOVERNMENT PROTECTIVE MARKING SCHEME	
Service Instruction	SI0818	PERSONNEL SECURITY	
Policy	STRPOL09 and associated SIs	Information Governance and Security	

Contact

Department	Email	Telephone ext.
Strategy and Performance	debbieappleton@merseyfire.gov.uk	4402

arget audience

All MFrS	X	Ops Crews		Fire safety		Community FS			
Principal officers		Senior officers		Non uniformed					

Relevant legislation (if any)

DRAFT - PROTECTIVE SECURITY POLICY

STRPOL14

1. Policy Introduction and Background

Protective Security is the term used to describe the actions/policies required to meet the threats to an organisation and to protect its assets from compromise. Protective Security is important when considering the political climate and the technology that poses threats and risks to the Fire and Rescue Authority. Effective security is important in maintaining the confidence of the public, staff, stakeholders and partner agencies in efficient, effective and safe service delivery.

Protective Security is a holistic process that covers three related aspects of security; information (documents/data systems), personnel (staff/customers) and physical (buildings/estates/property).

2. Policy Explanation

This Policy outlines Merseyside Fire and Rescue Authority's (MFRA) approach to implementing protective security. Implementation of this policy and the supporting guidance reinforces the importance of Protective Security within every aspect of MFRA. This will be achieved by integrating a number of complementary security measures to create an approach that includes all three aspects. The aim of the policy is to achieve compliance, as far as practicable, with the relevant aspects of HMG Security Policy Framework, and as detailed within the DCLG Fire & Rescue Protective Security Strategy.

Underpinning the Policy are a number of complementary Service Instructions (SI) that provide guidance and detail in respect of the three protective security requirements. This policy and supporting policies and SIs reflect national policy, codes of practice and guidance. Protective Security is a collective responsibility for all staff and failure to comply with the requirements of this policy and associated SIs may result in disciplinary action.

3. Policy Implementation

Protective Security – Objectives

Appropriate personnel security, secure information systems, and practical but robust physical security measures are the core components of a secure working environment. The aim is to identify and value the assets of the Authority, understand the threat and vulnerability to these assets, determine any impact from loss or compromise, and ensure robust, proportionate controls are implemented through continuous security review.

In order to comply with the Fire and Rescue Services Protective Security Strategy MFRA will continue to implement secure methods of working. This will be supported and verified by internal audits and regular staff training in order to satisfy stakeholders of our security compliance.

Governance, Risk Management and Compliance

The implementation and management of Protective Security is led by the Deputy Chief Fire Officer who is responsible for taking an organisational lead on all aspects of protective security. He is supported by officers who fulfil the following roles designated in the Fire and Rescue Services Protective Security Strategy:

Service Security Officer (SSO) – Group Manager Operational Preparedness - Responsible for exercising day to day responsibility for all aspects of protective security; physical, personnel and information

Information Technology Security Officer (ITSO) – ICT Applications Manager - Responsible for the security of information held in MFRA,s ICT systems

Senior Information Risk Owner (SIRO) – Director of Strategy and Performance - Responsible for owning MFRA information risks

Information Asset Owners (IAO)- Senior individuals in each department responsible for the security of individual information assets (eg. records, databases ICT systems).

These officers (and others) and this policy, establish a framework by which we will deliver an effective approach to Protective Security.

Integrated Protective Security

Information Security

Information is a key asset and its correct processing is vital to the delivery of services and the integrity of the organisation. MFRA must strike the right balance between sharing and protecting information and manage the impact and risks associated with maintaining the confidentiality, integrity and availability of all information. This includes marking documents in line with The Government Protective Marking Scheme, ICT related security and information audit and governance. This includes potential disciplinary or criminal proceedings for users whose actions compromise protectively marked information

Personnel Security

The purpose of Personnel Security is to provide a level of assurance as to the trustworthiness, integrity and reliability of Service employees, volunteers and contractors. As a minimum requirement all staff will be subject to recruitment controls known as the Baseline Personnel Security Standard. For more sensitive posts there are a range of security controls referred to as 'National Security Vetting'; these are designed to ensure that such posts are filled by individuals who are unlikely to be susceptible, for whatever reason or motive, to influence or pressure which might cause them to abuse their position.

All Departments will employ a risk management approach to Personnel Security to comply with protective security principles, seeking to reduce the risk of damage, loss, or compromise of Authority assets by the application of personnel security controls before and during employment. These controls do not provide a guarantee of reliability and must be supported by continuous and effective line management.

Physical Security

Providing an appropriate and proportionate range of measures to protect the Authority's buildings, estate, vehicles, equipment and other property is a key requirement of this Policy. Physical Security involves a number of distinct security measures which form part of a Service-wide approach to security that takes account of the balance between prevention, protection and response.

Associated Service Instructions [included in the document control sheet]

This page is intentionally left blank

Merseyside FIRE & RESCUE SERVICE

Service Instruction 0816

Protective Marking – Government Security Classifications and Government Protective Marking Scheme

Document Control

Description and Purpose

This document is intended to advise on the principles the Government Security Classifications (GSC) and their application in Merseyside Fire and Rescue Authority. It also (by way of an appendix) provides guidance on the previous marking system, the Government Protective Marking Scheme (GPMS).

Active date	Review date	Author	Editor	Publisher
28.02.14	28.02.15	Deb Appleton	Deb Appleton	Sue Coker

Permanent		Temporary		If temporary, review date must be 3 months or less.
	X			

Amendment History

Version	Date	Reasons for Change	Amended by
1.0	11.03.14	Update to information on draft version & following consultation	Deb Appleton

Risk Assessment (if applicable)

Date Completed	Review Date	Assessed by	Document location	Verified by(H&S)

Equalities Impact Assessment

Initial	Full	Date	Reviewed by	Document location
	X	21.10.2013	Wendy Kenyon	Strategy & Performance/EIAs/Approved for Publish

Civil Contingencies Impact Assessment (if applicable)

Date	Assessed by	Document location

Related Documents

Doc. Type	Ref. No.	Title	Document location
Policy	STRPOL14	Protective Security	Portal/Strategy & Performance/Polices & Service Instructions
Instruction	SI 0818	Personnel Security	Portal/Service Instructions
Policy	STRPOL09	Information Governance & Security Policy.	Portal/Strategy & Performance/Polices & Service Instructions
Instruction	SI 0675	Destruction of Confidential Waste	Portal/Service Instructions
Instruction	SI 0435	Data Protection Instructions	Portal/Service Instructions
Instruction	SI 0759	Destruction of Information Assets including Protectively Marked Information	Portal/Service Instructions

Contact

Department	Email	Telephone ext.
Strategy & Performance	debbieappleton@merseyfire.gov.uk	0151 296 4402

Target audience

All MFS	X	Ops Crews		Fire safety		Community FS			
Principal officers		Senior officers		Non uniformed					

Relevant legislation (if any)

INTRODUCTION

Purpose

This Service Instruction (SI) is to advise on the principles the Government Security Classifications (GSC) and their application in Merseyside Fire and Rescue Authority. It also (by way of an Appendix) provides guidance on the previous marking system, the Government Protective Marking Scheme (GPMS).

The Authority recognises that information and information systems are valuable assets, which play a major role in supporting the organisation's strategic objectives. Information security is important for ensuring the safe and secure transaction of information for Authority business and the success of carrying out policy and administrative activities.

Information is a key asset and its correct handling is vital to the delivery of Fire and Rescue Authority services and to the integrity of those services. To strike the right balance between sharing and protecting information, the Authority needs to manage the business impacts and information risks associated with:

- Confidentiality – protecting information from unauthorised access and disclosure;
- Integrity – safeguarding the accuracy and completeness of information and processing methods; and
- Availability – ensuring that information and associated services are only available to authorised users when required

Appropriate protection is required for all forms of information to ensure business continuity and to avoid breaches of the law and statutory, regulatory or contractual obligations.

Introduction to Government Security Classifications and Government Protective Marking

Protective marking of information assets is an important part of Protective Security (see STRPOL14 Protective Security and also **STRPOL009_Information Governance and Security Policy**) as allows a co-ordinated way of implementing an appropriate level of protective controls against the likely threat to sensitive information. The threat may be posed by many agents including criminals, investigative journalists, pressure groups and protesters, terrorists, hackers, computer malware (e.g. viruses), natural disasters and disgruntled OR dishonest Staff members. The pace of technological developments also means that organisations need to be ever aware of new risks and threats.

The GSC Policy is in force from 2nd April 2014 and this describes how HM Government classifies information assets to ensure they are appropriately protected and will be adopted by MFRA. It will replace the Government Protective Marking Scheme. After 2nd April 2014 the GSC markings need to be applied to information assets including, documents, electronic records, email and audio visual material. However, it is important that both systems are understood as some *GPMS information assets will still exist within the organisation after implementation of the GSC Policy. An aide memoire for dealing with GPMS marked information can be found at **Appendix 1**

*For clarification any information assets marked PROTECT; RESTRICTED; CONFIDENTIAL are using the GPMS markings. SECRET and TOP SECRET are used by both systems.

Government Security Classifications

Using a protective marking system ensures that a protective marking is applied to a sensitive information asset to indicate its value in terms of the damage that is likely to result from that information being compromised. Protective marking is underpinned by the principal that information is only made available to those with a legitimate 'Need to Know'

The purpose of protective markings is to indicate the value of a particular asset in terms of the damage that is likely to result from its compromise. The GSC System ensures that sensitive information receives a uniform level of protection and treatment across Government, according to its degree of sensitivity.

The Government Security Classifications streamline the classification for information assets into three types:

OFFICIAL

SECRET

TOP SECRET

The majority of information assets held within the Authority are unlikely to require a classification above OFFICIAL or OFFICIAL - SENSITIVE, but a very small number of departments may deal with information marked SECRET. It is unlikely that any will deal with TOP SECRET information. However, some individuals may be in receipt of information from other agencies that does contain these higher levels of marking. Information that has been obtained from sources, which are publicly available, will not require a protective marking.

This Protective Marking SI sets out appropriate measures through which the Authority will classify its information to facilitate the secure handling, storage and disposal of its information assets.

For a summary view of the requirements for marking and processing GSC marked information see **Appendix 2.**

Viewing a Protectively Marked information asset

To view any protectively marked information an individual must have: -

A Need to know - this means that you should only see information that is related to your work
The appropriate level of security clearance (for further information see **Service Instruction SI 0818 Personnel Security**

Marking an Information Asset

Protective Marking should be considered by all staff when they create an information asset (for example, a document) when they have received guidance on how to do so. Only the originating organisation can protectively mark an asset or change its protective marking, though holders of copies may challenge the level of protective marking applied. It is very important that, as an author, care be taken in selecting the appropriate protective marking. Information that is classified as OFFICIAL will not be physically marked, but OFFICIAL – SENSITIVE, SECRET and TOP SECRET information will require a marking.

Marking OFFICIAL - SENSITIVE, SECRET AND TOP SECRET: The latter two markings will be applied very rarely but OFFICIAL-SENSITIVE will be used more often. Any employees working with such documents can suggest a protective marking having applied the criteria, but the relevant Information Asset Owner and SMG member or Head of Department must approve that marking.

When protectively marking an asset, typically a document, it must be clearly and conspicuously marked. Mark each page at both the header and footer using bolded capital letters – for example **OFFICIAL - SENSITIVE**. File covers should be similarly marked. When marking e-mails put the marking in the subject or title box as well as in the message text, typically at the start or top of the e-mail.

Over classification should be avoided (eg classifying and marking a document as SECRET when it should be OFFICIAL and as a result, unmarked), as this risks introducing inefficiencies into the system, such as unnecessarily limiting access, increasing the costs of security controls needed to protect it and impairing business efficiency.

Equally, under classification should be avoided, which may put the asset at risk of accidental or deliberate compromise through inadequate protection.

Consider adding a time limit to the marking where the information asset will only require that marking for a short time, for example, information that is embargoed, but will be freely available once published.

Authors or owners of information assets should consider which of the following markings apply in every case and mark the asset accordingly.

Marking using the Government Security Classification

ALL routine public sector business, operations and services should be treated as **OFFICIAL**
The majority of information assets created by MFRA are likely to be at this level.
This includes a wide range of information, of differing value and sensitivity, which needs to be defended against threats such as activists, single-issue pressure groups, investigative journalists, competent individual hackers and the majority of criminal individuals and groups, and to comply with legal, regulatory and international obligations. This includes:

- The day to day business of MFRA,
- Public safety, criminal justice and enforcement activities.
- Many aspects of defence, security and resilience.
- Commercial interests, including information provided in confidence and intellectual property.
- Personal information that is required to be protected under the Data Protection Act (1998) or other legislation (e.g. health records).

OFFICIAL – SENSITIVE
This is subset of OFFICIAL is used by MFRA to mark assets that fall under the general classification of OFFICIAL but which require additional care in their handling and disclosure. These include:

- Very sensitive personal data. More routine personal data will be classified as OFFICIAL but in some cases may also carry a MFRA specific marking to indicate that it is required to be treated with confidentiality
- Commercial or marked sensitive information

In cases where OFFICIAL-SENSITIVE is considered the appropriate marking a descriptor can also be added to provide more information. For example “OFFICIAL-SENSITIVE Personal data” or “OFFICIAL-SENSITIVE commercial in confidence”.

SECRET

Very sensitive information that requires protection against threats such as sophisticated, well resourced and determined threat actors, such as some highly capable serious organised crime groups and some state actors.
and where the effect of accidental or deliberate compromise would be likely to result in any of the following:

a. Directly threaten an individual's life, liberty or safety (from highly capable threat actors).
b. Cause serious damage to the operational effectiveness or security of UK or allied forces such that in the delivery of the Military tasks:

    i. Current or future capability would be rendered unusable;
    ii. Lives would be lost; or,
    iii. Damage would be caused to installations rendering them unusable.

c. Cause serious damage to the operational effectiveness of highly valuable security or intelligence operations.
d. Cause serious damage to relations with friendly governments or damage international relations resulting in formal protest or sanction.
e. Cause serious damage to the safety, security or prosperity of the UK or friendly nations by affecting their commercial, economic and financial interests.
f. Cause serious damage to the security and resilience of Critical National Infrastructure (CNI) assets.
g. Cause major impairment to the ability to investigate or prosecute serious organised crime.

TOP SECRET
This reflects the highest level of capability deployed against the nation's most sensitive information and services. This covers exceptionally sensitive information assets that directly support (or threaten) the national security of the UK or allies **AND** require extremely high assurance of protection. This includes where the effect of accidental or deliberate compromise would be likely to result in any of the following:

a. Lead directly to widespread loss of life.
b. Threaten directly the internal stability of the UK or friendly nations.
c. Raise international tension.
d. Cause exceptionally grave damage to the effectiveness or security of the UK or allied forces, leading to an inability to deliver any of the UK Defence Military Tasks.
e. Cause exceptionally grave damage to relations with friendly nations.
f. Cause exceptionally grave damage to the continuing effectiveness of extremely valuable security or intelligence operations.

Storage of protectively marked information

Protectively marked information must not be left unattended during working hours when staff are away from their desks and are unable to lock the office/room. Protectively marked documents must not be taken out of the office unless appropriate security measures are in place. No protectively marked documents should be stored out of the office unless appropriate security containers and security alarms are fitted to the areas. The type of furniture needed to store protectively marked information in depends on the protective marking.

The following are minimum requirements:

Storage - Government Security Classifications

OFFICIAL

- Clear desk / screen policy
- Consider proportionate measures to control and monitor access to more sensitive assets
- Storage under single barrier and / or lock and key
- Consider use of appropriate physical security equipment / furniture (see the CPNI "Catalogue of Security Equipment", CSE)

SECRET

- Register and file documents in line with locally determined procedures
- Maintain appropriate audit trails
- Control use of photocopiers and multi-function digital devices in order to deter unauthorised copying or electronic transmission
- Limit knowledge of planned movements to those with a need to know
- Use of CPNI Approved Security Furniture
- Segregation of shared cabinets
- Proportionate measures to control and monitor access / movements

TOP SECRET

- Register movement of documents and undertake annual musters
- Conduct random spot checks of documents to ensure appropriate processing / handling / record keeping and record results
- Strictly limit knowledge of planned movements to those with a need to know
- Robust measures to control and monitor movements
- Information must be accountable

Electronic storage:

The security classification of electronic documents follows the same principles as that for hardcopy material and electronic documents must be protected in the same way.

Because of the differences between electronic and hardcopy documents, there are some extra steps needed to protect electronic data.

Protectively marked information on computer disk, CD, memory-stick or other electronic media must be marked with the security classification of the most highly classified data stored on the device. Protectively marked or sensitive information must only be stored on the MFRA network (subject to the restrictions outlined below) or on portable devices (such as memory sticks) provided by MFRA. This will ensure that sufficient levels of security are built in.

If there is a need to take protectively marked electronic documents away from the office, these must be protected in the same way as hardcopy material documents sharing the same classification. An encrypted device must be used for information marked at OFFICIAL- SENSITIVE

Electronic documents with a Government Protective Marking are also subject to Business impact Level restrictions:

The Business Impact levels

HMG IA Standard No.1 Business Impact Levels allow government organisations to consider the impact to business of unauthorised people; seeing information in a system (Confidentiality), changing information in a system (Integrity) and preventing access to information in a system (Availability).

For the previous Government Protective Marking Scheme there is a direct correlation between this and business impact level. The Government Protective Markings of PROTECT, RESTRICTED, CONFIDENTIAL, SECRET and TOP SECRET directly match to business impact levels 2, 3, 4, 5 and 6 respectively. This is a one-way relationship. It is not the case that an asset with a business impact level of 5 for confidentiality necessarily should be marked SECRET. This is especially true of impacts to aggregated data where large quantities of similar data are collected together and assigned an overarching impact level. In all cases, aggregation of significant amounts of data is likely to raise the impact level of its compromise.

The relevant business Impact Level for each of the Government Security Classifications has not been determined at time of writing. Until such a time as this is determined MFRA will assume that OFFICIAL could be IL2 or 3 and SECRET and TOP SECRET would be higher. As a result of current levels of network security, it would not be possible to store SECRET and TOP SECRET documents electronically on the network. Advice should be sought from the SIRO or Information Technology Security Officer.

MF&RS have controls in place: technical, people, policy, physical and assurance to handle information to BIL2 (Business Impact Level 2) – PROTECT.

There are risks associated with storing RESTRICTED Information on the existing MFRA network, sending it using MFRA Corporate E-Mail or accessing it on a USB stick from any MFRA PC or Laptop or indeed and PC or LAPTOP that has not been IL3 cleared. All systems at a level of BIL 3 or above must be formally accredited to HMG Information Assurance Standard No.2 (IS2). However the Authority does receive RESTRICTED information and it has been agreed that it can be held on the network as an interim solution. As soon as a BIL3 solution is available or the Business Impact Levels for the GSC have been published the situation will be reviewed. The exception to this is RESTRICTED information relating to national and local resilience which can be held on the National Resilience Extranet (NRE), an online private 'network' designed to enable civil protection practitioners to work together for emergency planning and incidents.

Communicating and Sharing Protectively Marked Information

Government Security Classifications

Email

OFFICIAL

- Information in transit between Government or other trusted organisations will be via accredited shared infrastructure (such as PSN) or protected using Foundation Grade encryption.
- Information may be emailed / shared unprotected to external partners / citizens, subject to local business policies and procedures
- Where more sensitive information must be shared with external partners (e.g. citizens), consider using secure mechanisms (e.g. browser sessions using SSL / TLS

SECRET

- Electronic information will only be exchanged via appropriately secured mechanisms. This will involve use of appropriately accredited shared services or (revitalised) Enhanced Grade encryption
- Information will only be shared with defined users on appropriate and accredited recipient ICT systems

TOP SECRET

- Electronic information will only be exchanged via appropriately secured mechanisms. This will involve use of appropriately accredited shared services or High Grade encryption
- Information will only be shared with defined users on appropriate and accredited recipient ICT systems.

Removable media

OFFICIAL

- The use of removable media will be minimised, and other approved information exchange mechanisms should be used where available in preference
- Any information moved to or transferred by removable media must be minimised to the extent required to support the business requirement. Any removable media (eg a memory stick) must be encrypted and purchased through the ICT help desk. Encryption helps to protect the content, particularly where it is outside the organisation's physical control

SECRET

- Content must be appropriately encrypted unless (by exception) there exists appropriate full life physical protection

TOP SECRET

- Content must be appropriately encrypted unless (by exception) there exists appropriate full life physical protection

Telephone

OFFICIAL

- Details of sensitive material should be kept to a minimum.
- Recipients should be waiting to receive faxes containing personal data and / or data marked with the OFFICIAL – SENSITIVE caveat.

SECRET

- Secure Telephony, VTC and secure fax

TOP SECRET

- Secure Telephony, VTC and secure fax

Post

OFFICIAL

- Include return address, never mark classification on envelope
- Consider double envelope for sensitive assets
- Consider using registered Royal Mail service or reputable commercial courier's "track and trace" service

SECRET

- Local Management approval required, actions recorded in document movement register
- Robust double cover
- Approved registered mail service commercial courier ("track and trace"), or Government courier

TOP SECRET

- Security cleared (DV) diplomatically accredited courier only

Destruction of Protectively Marked Documents

Protectively marked documents should be reviewed regularly (ideally annually) to check whether they are still required. The relevant Retention Schedule should be consulted. Contact recordsmanagement@merseyfire.gov.uk for more information or refer to **Service Instruction 0687**. If a document is no longer required it should be destroyed using the right method for its classification, making sure that no one will be able to put it back together to read it. Consult **Service Instruction 0759 Destruction of Information Assets Waste including Protectively Marked Information** for more information.

If the information asset did not originate in MFRA the document should be returned to the provider or originator when it is no longer required (see section 5 above).

The way the document is destroyed will depend on its classification: -

Government Security Classifications

OFFICIAL
Dispose of with care using approved commercial disposal products to make reconstitution unlikely (refer to Centre for the Protection of National Infrastructure (CPNI) guidance and HMG IS5 Government guidance). Strategy and Performance Function will ensure that current arrangements are compliant and only suitable disposal products (eg cross cut shredders) will be available for purchase.

SECRET

- Consult the Senior Information Risk Owner (SIRO) - Verify document is complete before destruction
- Use Government approved equipment and or service providers.

TOP SECRET

- Consult the SIRO - Control measures will be used to witness and record destruction

Information losses/breaches

Any officer who becomes aware of the loss, theft or otherwise inappropriate disclosure of information marked OFFICIAL – SENSITIVE (Government Security classifications) or PROTECT or RESTRICTED (Government Protective Marking Scheme) should follow the process outlined in **Appendix 3**

Where the information asset is marked as CONFIDENTIAL, SECRET, TOP SECRET a different procedure must be followed. This is also outlined in **Appendix 3**.

Appendix 3 also contains details of the relevant Protective Security roles and the holders of those roles.

All reported breaches or potential weaknesses are investigated and, where necessary, further or alternative measures will be introduced to secure data. Such reports will be received by the Senior Information Risk Owner, the appropriate department head as necessary and in some cases, Government departments or the Police.

Disciplinary action could be taken depending on the circumstances of the loss or breach.

APPENDIX 1 - Aide Memoire for handling information marked using the Government Protective Marking Scheme

Storage of protectively marked information

Protectively marked information must not be left unattended during working hours when staff are away from their desks and are unable to lock the office / room. Protectively marked documents must not be taken out of the office unless appropriate security measures are in place. No protectively marked documents should be stored out of the office unless appropriate security containers and security alarms are fitted to the areas.

The type of furniture you need to store protectively marked information in depends on the protective marking. The following are minimum requirements:

PROTECT and RESTRICTED can be stored in any lockable furniture, within a secure building.

CONFIDENTIAL and SECRET must be stored in furniture locked with specific security keys or combinations as approved by Security Equipment Approved Panel (SEAP).

TOP SECRET documents must be stored in furniture locked with specific security devices, within a lockable room, with only a limited number of people permitted access to the room keys.

TOP SECRET and SECRET documents must be filed in numbered files or containers. It is useful to add a note of the file's contents so that individual files can be readily accessed when needed.

The security classification of electronic documents follows the same principles as that for hardcopy material and electronic documents must be protected in the same way. Most IT systems are not accredited to carry material protectively marked above PROTECT or RESTRICTED, and responders are encouraged to confirm with their information security officer the classification of material that may be stored on their system. Because of the differences between electronic and hardcopy documents, there are some extra steps needed to protect electronic data:

- Protectively marked information on computer disk, CD, memory-stick or other electronic media must be marked with the security classification of the most highly classified data stored on the device.
- Protectively marked or sensitive information must not be saved on a palm-held computer (PDA) ar a tablet unless provided by MFRA for the purpose.
- If there is a need to take protectively marked electronic documents away from the office, these must be protected in the same way as hardcopy material documents sharing the same classification.

Communicating and Sharing Protectively Marked Information

Email

There are specific rules for sending protectively marked information by email: -

Generally, NOT PROTECTIVELY MARKED and most PROTECT material may be transmitted across any internet email system. Where sensitive personal data (especially in aggregate) or material marked “PROTECT – PERSONAL DATA” is being sent by email, this data should be commercially encrypted (up to FIPS 140 standard). Email accounts that contain ‘gsi’ or ‘pnn’ in the address meet this standard.

Up to RESTRICTED may be sent between two systems accredited to communicate at this level (i.e.username@organisation.gsi.gov.uk to username@organisation.pnn.police.uk). If only one party has the necessary accredited system, then up to PROTECT only may be sent (subject to the caveat above regarding sensitive personal data).

Telephone

When you are dealing with information protectively marked RESTRICTED or above, you should not:

- Talk about it over a non-secure telephone line or non-secure mobile phone (unless it is RESTRICTED and your organisation has accepted the risk of so doing);
- Send it over a non-secure fax line (as above in regard RESTRICTED); or send it to a pager.

NOT PROTECTIVELY MARKED and PROTECT may be discussed / sent over non secure telephone / fax lines.

Post

A return address should always be included when sending protectively marked information by post. This is because all undelivered mail without a return address is opened at a Royal Mail sorting office where staff are not security cleared. The specific procedures for sending PROTECT, RESTRICTED and CONFIDENTIAL documents by post are:

- **PROTECT / RESTRICTED:** Address the envelope to an individual by name or job title and mark it 'Addressee only'. Do not include the classification on the envelope.
- **CONFIDENTIAL:** Follow the guidelines for RESTRICTED documents. When sending away from the building, the envelope must be marked CONFIDENTIAL and placed in a second envelope. Do not include the classification on the outer envelope.
- **SECRET / TOP SECRET:** Follow the guidelines for CONFIDENTIAL documents. Trusted hand delivery and special courier should be used for mail purposes.

Destruction of Protectively Marked Documents

You should review protectively marked documents regularly (ideally annually) to check whether you still need to keep them. If you no longer need a document, you should destroy it using to the right method for its classification, making sure that no one will be able to put it back together to read it. You should also record it in a registry (CONFIDENTIAL and higher). Alternatively, arrange for the document to be returned to the provider or originator.

The way you destroy the document will depend on its classification: -

- **PROTECT and RESTRICTED:** Use a cross cut shredder or put your documents in a confidential waste sack that is collected by an approved waste collector. This will make it unlikely that anyone will be able to read the information.
- **CONFIDENTIAL:** Tear up documents and place them in a confidential waste sack that is collected by an approved waste collector. Alternatively, shred as SECRET.
- **SECRET:** The documents should be shredded in a cross cutter; put the paper in at right angles to the print. The size of the shredded strips should be no more than 0.8mm and 12mm and not show more than two characters side by side. This will make it highly unlikely that anyone can put the document back together. When destroying SECRET documents, a record must be retained

of the date the document was destroyed and who authorised its destruction. This record must be kept for five years.

- **TOP SECRET:** These documents must be destroyed in the same way as SECRET documents, except that two people must witness the shredding and sign the registry.

Also consult the MFRS **Service Instruction SI 0675 Destruction of Confidential Waste**

http://intranetportal/sites/cc/Service%20Instructions1/Service%20Instructions/SI%200675%20Destruction%20of%20Confidential%20Waste.doc

HMG IA Standard No. 5 - Secure Sanitisation also provides comprehensive guidance

APPENDIX 2 - Government Security Classifications – Matrix V1.0

	OFFICIAL	OFFICIAL - SENSITIVE	SECRET	TOP SECRET
Overview	The majority of information that is created or processed by the public sector. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile.		Very sensitive information that justifies heightened protective measures to defend against determined and highly capable threat actors. For example, where compromise could seriously damage military capabilities, international relations or the investigation of serious organised crime.	The most sensitive information requiring the highest levels of protection from the most serious threats. For example, where compromise could cause widespread loss of life or else threaten the security or economic wellbeing of the country or friendly nations.
Threat Profile	Similar to that faced by a large UK private company with valuable information and services. It anticipates the need to defend data or services against compromise by attackers with bounded capabilities and resources. This may include (but is not limited to) hactivists, single-issue pressure groups, investigative journalists, competent individual hackers and the majority of criminal individuals and groups. Many Government agencies and public sector organisations will operate exclusively at this level		This anticipates the need to defend against a higher level of capability than would be typical for the OFFICIAL level. This includes sophisticated, well-resourced and determined threat actors, such as some highly capable serious organised crime groups and some state actors. Reasonable steps will be taken to protect information and services from compromise by these actors, including from targeted and bespoke attacks.	This reflects the highest level of capability deployed against the nation's most sensitive information and services. It is assumed that advanced state actors will prioritise compromising this category of information or service, using significant technical, financial and human resources over extended periods of time. Highly bespoke and targeted attacks may be deployed, blending human sources and actions with technical attack. Very little information risk can be tolerated.
Definition	ALL routine public sector business, operations and services should be treated as OFFICIAL. This includes: • The day to day business of government, service delivery and public finances. • Routine international relations and diplomatic activities. • Routine public safety, criminal justice and enforcement activities. • Many aspects of defence, security and resilience. • Routine commercial interests and information • Personal information that is required to be protected under the	A limited subset within OFFICIAL with more damaging consequences (individual or organisational) if compromised. The risk must be clear and justifiable, including: • Most sensitive corporate or operational information (e.g. organisational change planning, contentious negotiations, major security or business continuity) • Commercial or market sensitive information, including that subject to statutory or regulatory obligations • Information about investigations and civil or criminal proceedings	Very sensitive information where the effect of accidental or deliberate compromise would be likely to result in any of the following: • Directly threaten an individual's life, liberty or safety (from highly capable threat actors). • Cause serious damage to the operational effectiveness or security of UK or allied forces. • Cause serious damage to the operational effectiveness of highly valuable security or intelligence operations. • Cause serious damage to relations with friendly governments or	Exceptionally sensitive information assets that directly support (or threaten) the national security of the UK or allies. This includes where the effect of accidental or deliberate compromise would be likely to result in any of the following: • Lead directly to widespread loss of life. • Threaten directly the internal stability of the UK or friendly nations. • Raise international tension. • Cause exceptionally grave damage to the effectiveness or security of the UK or allied forces,

	OFFICIAL	OFFICIAL - SENSITIVE	SECRET	TOP SECRET
	Data Protection Act (1998) or other legislation (e.g. health records).	that could compromise public protection, enforcement, or prejudice justice • More sensitive information about defence or security assets or equipment that could damage capabilities or effectiveness, but not appropriate for SECRET protections • Very sensitive personal data, that may have severely damaging consequences through loss, but not required to manage as SECRET	damage international relations resulting in formal protest or sanction. • Cause serious damage to the safety, security or prosperity of the UK or friendly nations by affecting their commercial, economic and financial interests. • Cause serious damage to the security and resilience of Critical National Infrastructure (CNI) assets. • Cause major impairment to the ability to investigate or prosecute serious organised crime.	leading to an inability to deliver any of the UK Defence Military Tasks. • Cause exceptionally grave damage to relations with friendly nations. • Cause exceptionally grave damage to the continuing effectiveness of extremely valuable security or intelligence operations. • Cause long term damage to the UK economy. • Cause major, long-term impairment to the ability to investigate or prosecute serious organised crime.
Personnel Security	• Appropriate recruitment checks (e.g. the BPSS, or equivalent) • Reinforce personal responsibility and duty of care through training	• BPSS as minimum for regular, uncontrolled access • 'Need to Know' principle applied	• Always enforce 'Need to Know' • SC for regular, uncontrolled access • Special Handling Instructions	• DV for regular, uncontrolled access
Handling	• General good practice approach such as clear desk / screen policy	• Consider proportionate measures to control and monitor access	• Register and file documents in line with locally determined procedures • Maintain appropriate audit trails • Control use of photocopiers and multi-function digital devices in order to deter unauthorised copying or electronic transmission • Limit knowledge of planned movements to those with a need to know	• Register movement of documents and undertake annual musters • Conduct random spot checks of documents to ensure appropriate processing / handling / record keeping and record results • Strictly limit knowledge of planned movements to those with a need to know
Storage	• General good practice administration should apply • Storage under single barrier and / or lock and key where possible	• Protect by single barrier and / or lock and key as minimum • Consider use of appropriate physical security equipment / furniture	• Use of CPNI Approved Security Furniture (SAPMA required) • Segregation of shared cabinets • Proportionate measures to control and monitor access / movements	• Use of CPNI Approved Security Furniture (SAPMA required) • Robust measures to control and monitor movements • Information must be accountable
Movement	• Single cover • Precautions against overlooking when working in transit • Authorisation required for significant volume of records/files	• Single cover • Precautions against overlooking when working in transit • Authorisation required for significant volume of records/files	• Risk assess the need for two people to escort the movement of document(s)/media • Documented local management approval required and completion	• Senior Manager approval subject to risk assessment

	OFFICIAL	OFFICIAL - SENSITIVE	SECRET	TOP SECRET
			of document / media removal / movement register • Sealed tamper-evident container / secure transportation products (refer to CSE) • Not accessed in public areas	
Transfer	• Post or courier • Include return address, never mark classification on envelope	• Post or courier • Consider use of double envelope (protective marking on inner, return address on outer) • Consider using registered Royal Mail service or reputable commercial couriers 'track and trace' service	• Local Management approval required, actions recorded in document movement register • Robust double cover • Approved registered mail service commercial courier - 'track and trace' service	• Senior Manager approval subject to risk assessment • Special handling arrangements may need to be considered
Telephony, Video, Fax and Airwave	• Routine good administration applies	• Details should be kept to a minimum (use of guarded speech) • Recipients should be waiting to receive faxes • Airwave is appropriately encrypted	• Secure Telephony, VTC and secure fax (BRENT)	• Secure Telephony, VTC and secure fax (BRENT)
Electronic Information at Rest	• Protected at rest by default (commercially available, appropriately assured, security products) • May be appropriate physical protection (such as data centre) or may involve Foundation Grade data at rest encryption	• Data at rest on non-physically secure devices will be encrypted with Foundation Grade protection or other suitably assured products	• Protected at rest by physical security appropriate for SECRET assets (SAPMA required) • Data at rest on non-physically secure devices will be encrypted with (revitalised) Enhanced Grade protection	• Protected at rest by physical security appropriate for TOP SECRET assets (SAPMA required) • Data at rest on non-physically secure devices will be encrypted with High Grade protection
Electronic Information in Transit	• Information may be emailed / shared unprotected to external partners / citizens (subject to local business policies and procedures) • Personal information should be encrypted (essential in aggregate)	• Via accredited shared infrastructure (such as PSN), protected using Foundation Grade encryption, or other approved encryption product must be used (CJSM/NRE etc.) • Use secure mechanisms, such as client-side encryption or browser sessions using SSL / TLS	• Electronic information will only be exchanged via appropriately secured mechanisms. This will involve use of appropriately accredited shared services or (revitalised) Enhanced Grade encryption • Information will only be shared with defined users on appropriate and accredited recipient ICT systems	• Electronic information will only be exchanged via appropriately secured mechanisms. This will involve use of appropriately accredited shared services or High Grade encryption • Information will only be shared with defined users on appropriate and accredited recipient ICT systems
Removable Media	• Any information moved to or transferred by removable media should be minimised to the extent required to support the business	• Appropriate encryption should be used for temporary occasions • Appropriate encryption must be	• Content must be appropriately encrypted unless (by exception) there exists appropriate full life physical protection	• Content must be appropriately encrypted unless (by exception) there exists appropriate full life physical protection

	OFFICIAL	OFFICIAL - SENSITIVE	SECRET	TOP SECRET
	requirement • Consider appropriate encryption to protect the content, particularly where it is outside the organisations physical control	used for permanent / semi-permanent use		

APPENDIX 3 – Process for handling information losses/breaches (including inappropriate disclosure of information)

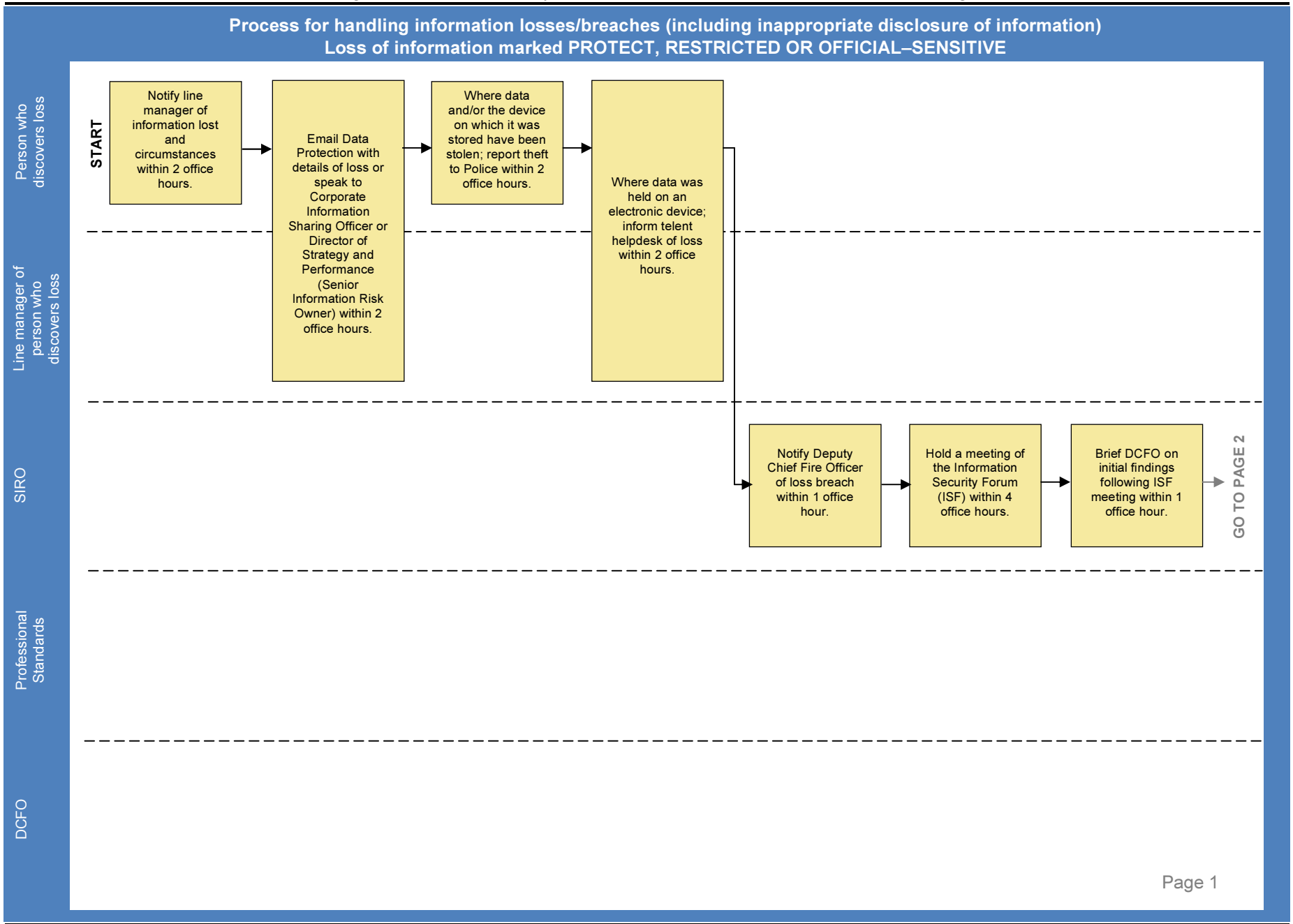
Also see Service instruction SI 0435 Data Protection Instructions

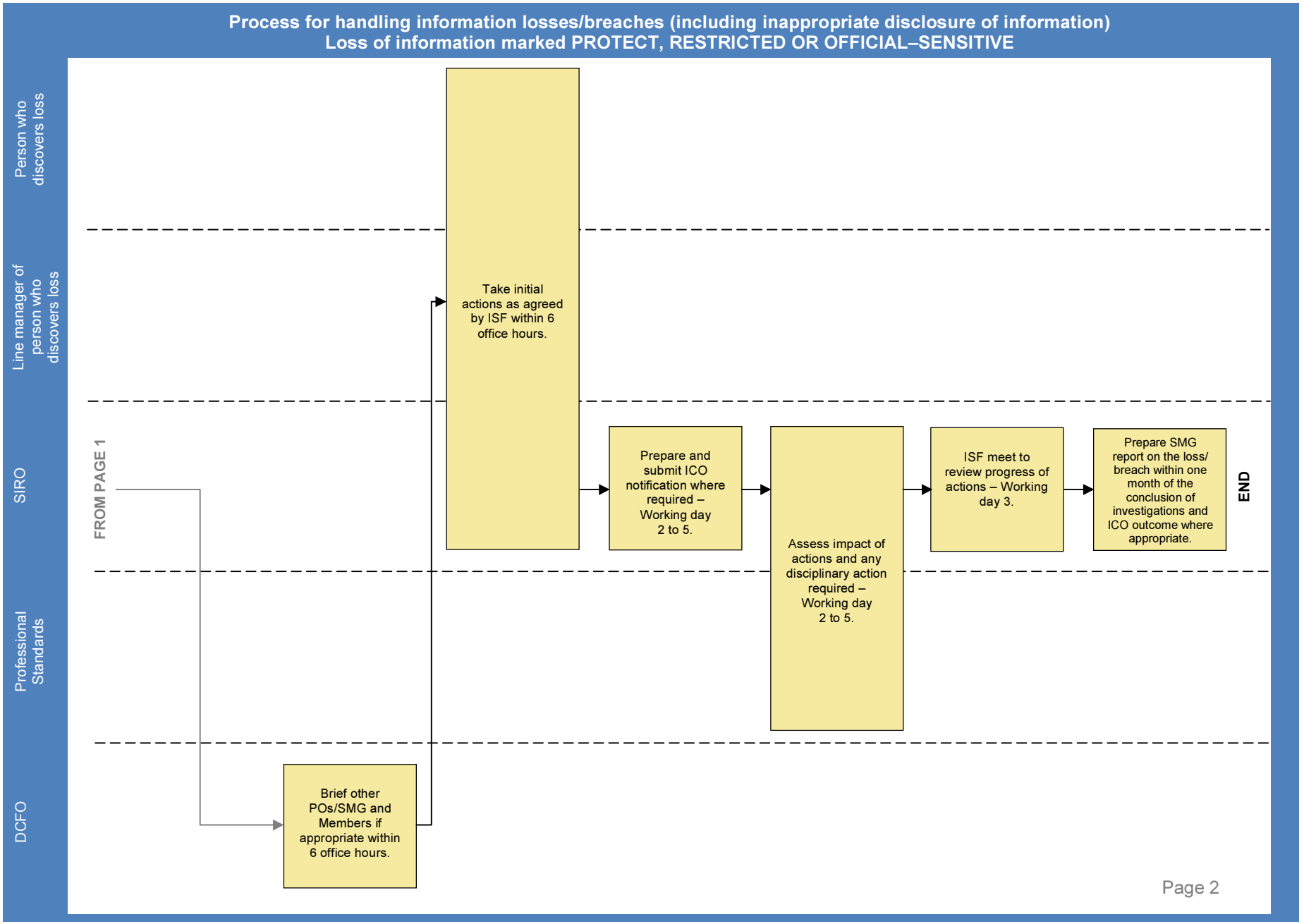
*Office hours. Out of hours response will be considered on a case by case basis

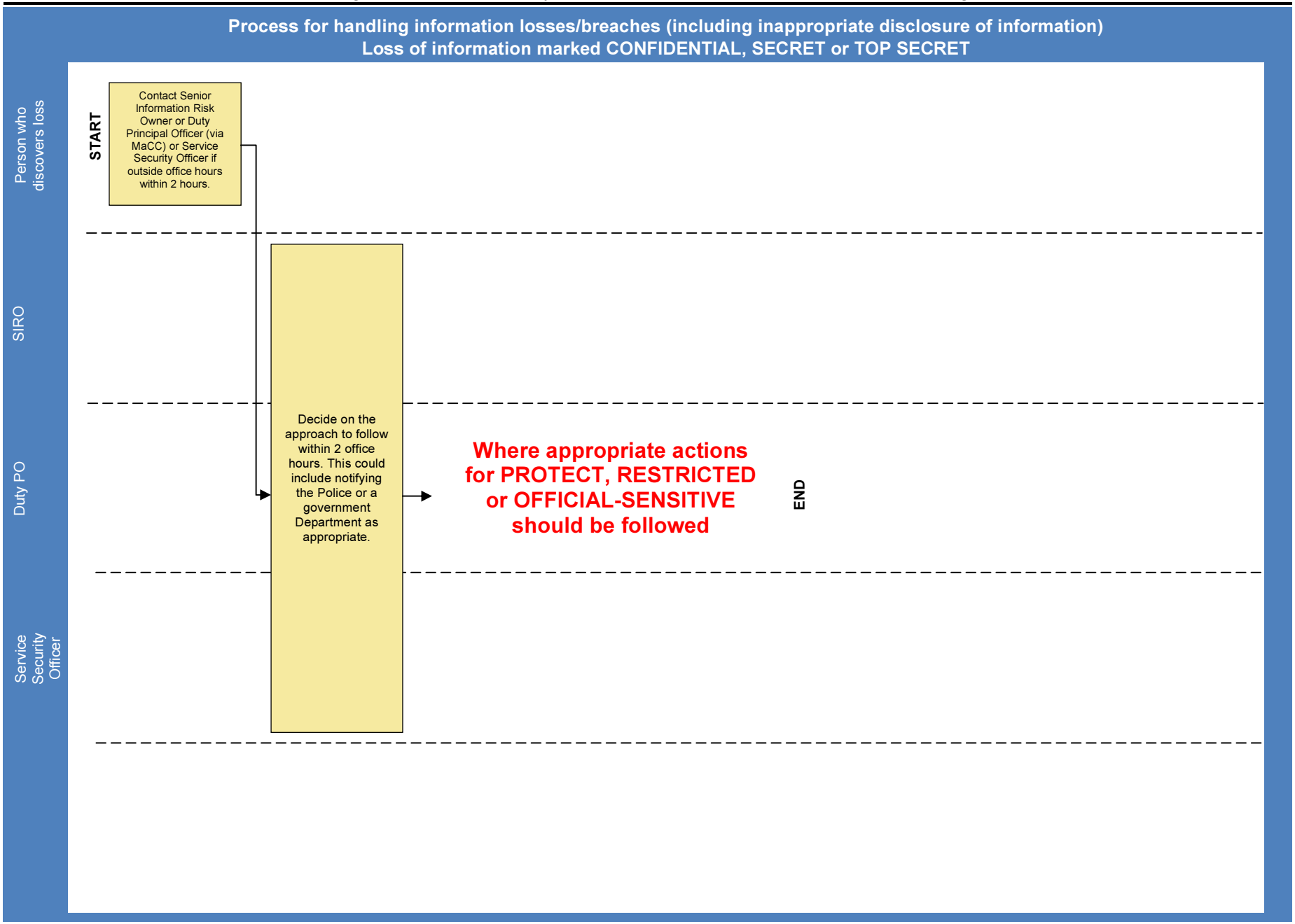
Loss of information marked PROTECT, RESTRICTED OR OFFICIAL - SENSITIVE			
	Action	**Responsible person**	**Timescale**
1	Notify line manager of the information lost and the circumstances	Person who discovers the loss	At the first opportunity following discovery of the loss – within *2 hours
2	Either Email dataprotection@merseyfire.gov.uk with details of the loss or ring 0151 296 4479/4474 and speak to the Corporate Information Sharing Officer or 07818 034982 for the Director of Strategy and Performance (Senior Information Risk Owner)	Person who discovers the loss or their line manager	At the first opportunity following discovery of the loss – *2 hours
3	Where the data and/or the device on which it was stored have been stolen; report the theft to the Police.	Person who discovers the loss	At the first opportunity following discovery of the loss – within *2 hours
4	Where the data was held on an electronic device; contact the telent helpdesk to inform them of the loss	Person who discovers the loss or their line manager	At the first opportunity following discovery of the loss – within *2 hours
5	Senior Information Risk Owner (SIRO) notifies the Deputy Chief Fire Officer of the loss breach	SIRO	At the first opportunity following notification – within *1 hour
6	SIRO holds a meeting of the Information Security Forum (ISF) to consider the following: • What has been lost – are further investigations necessary (Service Security Officer to be involved)?	SIRO	Within *4 hours of notification

	• whether the information "belongs" to MFRA • Potential damage to the organisation concerned or individuals and how they will be informed • Is notification to the Information Commissioners Office (ICO) required? • Is there an insurance implication? • What immediate message needs to be sent to staff/public (Corporate Communications to be advised) • Consider level of police involvement		
7	SIRO briefs the DCFO on the initial findings	SIRO/DCFO	Following ISF meeting – within *1 hour
8	DCFO briefs other POs/SMG and Members if appropriate	DCFO/SIRO	Within *6 hours of notification
9	SIRO and notifying officer/line manager take initial actions as agreed by ISF	SIRO/notifying officer/ line manager	Start within *6 hours of notification
10	SIRO prepares and submits ICO notification where required	SIRO	Day *2 to 5
11	SIRO assesses impact of actions and any disciplinary action required – with Professional Standards.	SIRO/Professional Standards	Day *2 to 5
12	ISF meets to review progress of actions	SIRO	Day *3
13	SIRO prepares SMG report on the loss/ breach	SIRO	Within one month of the conclusion of investigations and ICO outcome where appropriate

Loss of Information marked CONFIDENTIAL, SECRET or TOP SECRET			
	Action	**Responsible person**	**Timescale**
1	Contact the Senior Information Risk Owner or Duty Principal Officer (via MaCC) or Service Security Officer if outside office hours.	Person who discovers the loss	At the first opportunity following discovery of the loss – within 2 hours
2	A decision will then be taken on the approach to follow. This could include notifying the Police or a government Department as appropriate.	SIRO/Duty PO/Service Security Officer	Within 2 hours of notification
3	Where appropriate, the above actions for PROTECT, RESTRICTED or OFFICIAL-SENSITIVE will be followed in addition to any specific actions determined in 3.	SIRO	In accordance with timescale for PROTECT, RESTRICTED and OFFICIAL-SENSITIVE
	Protective Security roles: **Protective Security Lead** Phil Garrigan - Deputy Chief Fire Officer **Service Security Officer** (SSO) - (TBC) **Information Technology Security Officer** (ITSO) - Mark Hulme – ICT Applications Manager **Senior Information Risk Owner** (SIRO) Deb Appleton – Director of Strategy and Performance **Information Asset Owners** (IAO) – there is at least one IA in each department. Contact the SIRO for further details		


Process for handling information losses/breaches (including inappropriate disclosure of information)
Loss of information marked PROTECT, RESTRICTED OR OFFICIAL–SENSITIVE
Person who discovers loss
Line manager of person who discovers loss
SIRO
Professional Standards
DCFO
START
Notify line manager of information lost and circumstances within 2 office hours.
Email Data Protection with details of loss or speak to Corporate Information Sharing Officer or Director of Strategy and Performance (Senior Information Risk Owner) within 2 office hours.
Where data and/or the device on which it was stored have been stolen; report theft to Police within 2 office hours.
Where data was held on an electronic device; inform telent helpdesk of loss within 2 office hours.
Notify Deputy Chief Fire Officer of loss breach within 1 office hour.
Hold a meeting of the Information Security Forum (ISF) within 4 office hours.
Brief DCFO on initial findings following ISF meeting within 1 office hour.
GO TO PAGE 2
Page 1


Process for handling information losses/breaches (including inappropriate disclosure of information)
Loss of information marked PROTECT, RESTRICTED OR OFFICIAL–SENSITIVE
Person who discovers loss
Line manager of person who discovers loss
SIRO
Professional Standards
DCFO
FROM PAGE 1
Take initial actions as agreed by ISF within 6 office hours.
Prepare and submit ICO notification where required – Working day 2 to 5.
Assess impact of actions and any disciplinary action required – Working day 2 to 5.
ISF meet to review progress of actions – Working day 3.
Prepare SMG report on the loss/ breach within one month of the conclusion of investigations and ICO outcome where appropriate.
END
Brief other POs/SMG and Members if appropriate within 6 office hours.
Page 2


Process for handling information losses/breaches (including inappropriate disclosure of information)
Loss of information marked CONFIDENTIAL, SECRET or TOP SECRET
Person who discovers loss
SIRO
Duty PO
Service Security Officer
START
Contact Senior Information Risk Owner or Duty Principal Officer (via MaCC) or Service Security Officer if outside office hours within 2 hours.
Decide on the approach to follow within 2 office hours. This could include notifying the Police or a government Department as appropriate.
Where appropriate actions for PROTECT, RESTRICTED or OFFICIAL-SENSITIVE should be followed
END

Service Instruction 0818
Personnel Security

Document Control

Description and Purpose

This document is intended to ensure compliance with the requirements of Her Majesty's Government's (HMG) Security Policy Framework and to safeguard Authority information and assets

Active date	Review date	Author	Editor	Publisher
28.02.14	28.02.15	Vicky Walsh	Suzanne Lea	Sue Coker

Permanent	X	Temporary		If temporary, review date must be 3 months or less.

Amendment History

Version	Date	Reasons for Change	Amended by
1.0	11.03.14	Update to information on draft version	Deb Appleton

Risk Assessment (if applicable)

Date Completed	Review Date	Assessed by	Document location	Verified by(H&S)

Equalities Impact Assessment

Initial	Full	Date	Reviewed by	Document location
	X	21.01.14	Wendy Kenyon	Strategy & Performance/EIA's/Approved for Publish 2014

Civil Contingencies Impact Assessment (if applicable)

Date	Assessed by	Document location

Related Documents

Doc. Type	Ref. No.	Title	Document location
Policy	STRPOL14	Protective Security	TBC
Policy	TBC	Recruitment & Selection	TBC
Policy	STRPOL09	Information Governance & Security	Portal
Instruction	SI 0816	Protective Marking – Government Security Classifications and Government Protective Marking Scheme	
Instruction	SI 0759	Destruction of information Assets Including Protectively Marked Information	Portal
Instruction	SI 0435	Data Protection Instructions	Portal
Instruction	SI 0718	Security of Premises and Terrorist Threats	Portal

Contact

Department	Email	Telephone ext.
People & Organisational Development	Contracts&PolicyTeam@merseyfire.gov.uk	0151 296 4360

Target audience

All MFS	x	Ops Crews		Fire safety		Community FS			
Principal officers		Senior officers		Non uniformed					

Relevant legislation (if any)

Data Protection Act (DPA) (1998) **Employment Rights Act (1996)** **Equality Act (2010)** **Human Rights Act (1998)** **Immigration Asylum and Nationality Act (2006)** **Rehabilitation of Offenders Act (1974) and the Rehabilitation of Offenders (Northern Ireland) Order (1974)** **Trade Union Reform and Employment Rights Act (1993)**

INTRODUCTION

The aim of this document is to ensure compliance with the requirements of Her Majesty's Government's (HMG) Security Policy Framework and to safeguard Authority information and assets.

Personnel Security provides a level of assurance as to the trustworthiness, integrity and reliability of all Authority staff. As a minimum requirement all staff will be subject to recruitment controls known as baseline personnel security standard.

For more sensitive posts there is a range of security controls referred to as 'National Security Vetting'; these are specifically designed to ensure that such posts are filled by individuals who are unlikely to be susceptible, for whatever reason or motive, to influence or pressure which might cause them to abuse their position.

These controls "whilst ensuring a degree of risk management" do not provide a guarantee of reliability and must be supported by continuous and effective line management and aftercare arrangements.

Purpose

The purpose of Personnel Security is to provide an acceptable level of assurance as to the integrity of all Authority staff and contractors who are to be given authorised access to buildings, information or other assets belonging to or entrusted to the Authority including the Joint Control Centre. This service instruction aims to ensure that individuals, who need access to such assets in order to carry out their roles, are less likely to be susceptible, for whatever reason or motive, to temptation or pressure that could cause them to abuse the access they have been given.

Review

This policy will be reviewed periodically to ensure uniformity of treatment and justice for all employees in the implementation of the Authority's procedures and to ensure compliance with relevant legislation.

Equality and diversity

Employees must ensure that they treat other employees, Members, Service users and other people with whom they come into contact during their work in a way that complies fully with the Equality Act 2010 and does not discriminate against individuals or groups on the grounds of any protected characteristics.

Applicability

This service instruction will apply to all existing Authority staff, prospective employees, contractors, volunteers and any other similar organisations and will also incorporate the Authority's **Recruitment and Selection policy**.

For the purposes of this procedure the definition of Authority staff applies to:

- substantive
- fixed term
- Part time/full time
- Secondees
- Agency staff
- Work experience/placements

*Please note this list is not exhaustive

General principles

- Before any individual can start employment with the Authority or work on Authority premises, the appropriate level of personnel security must be granted. All candidates must go through a basic disclosure and, dependent upon their role and location, may also go through Police Vetting and/or National Security Vetting.
- Personnel security is a pre-requisite for employment and therefore those who refuse to support the process will not be considered.
- The level of personnel security will be determined by the requirements of the role and will take into account the extent to which unsupervised access to premises, personnel, computer systems and data is required.
- Should an employee change location or role then the appropriate level of personnel security must be granted prior to commencement.

Personnel security risk assessment

In order to rationalise what security controls might be appropriate for particular posts within the Authority, a risk assessment will be conducted. The risk assessment will consider the operating environment of the site, the level of access available to post holders and the potential risk those posts pose to sensitive material, valuable assets and operational capability. Such an assessment will ensure that any proposed security controls, such as the level of screening applied to certain posts, is proportionate and appropriate.

Levels of personnel security screening

There are three levels of personnel security screening within the Authority.

1. Baseline Personnel Security Standard (BPSS)
2. Non-Police Personnel Vetting Level Three (NPPV3)
3. National Security Vetting (NSV) – 3 levels
    a. Counter Terrorism Check (CTC)
    b. Security Check (SC)
    c. Developed Vetted (DV)

General roles and positions

The table below reflects the general roles and positions that are pre-determined generically as requiring particular security controls within the Authority.

Role	Security Control
All Authority staff, prospective employees, contractors, FireFit HUB, Fire Support Network (FSN) and any other similar organisations unless they are required to have NPPV3 for their role which supersedes BPSS	Baseline Personnel Security Standard (BPSS)
All Authority staff, prospective employees, contractors, volunteers and any other similar organisations that require as part of their role or location of work to have access to the Joint Control Centre.	Non-Police Personnel Vetting Level Three (NPPV3)
Brigade Manager	Security Check (SC)
CBRN Silver/Gold Commander	Security Check (SC)
National Interagency Liaison Officer (NILO)	Security Check (SC)
National Resilience Assurance Team	Security Check (SC)

*Please note this list is not exhaustive.

1. BASELINE PERSONNEL SECURITY SCREENING (BPSS)

The Baseline Personnel Security Standard provides a sensible, and in the case of National Security Vetting essential, grounding for making informed employment decisions. The majority of the checks conducted to form a Baseline Personnel Security Standard are mandated by law, such as the confirmation of Nationality and Immigration status.

Those who are cleared to Baseline Personnel Security Standard level may have frequent access up to CONFIDENTIAL, and occasional controlled access to SECRET material as defined in the Government Protective Marking System.

The Baseline Personnel Security Standard is not a formal security clearance within National Security Vetting, but is designed to provide a level of assurance as to the trustworthiness and integrity of individuals whose work, in the main, involves uncontrolled access to, or knowledge or custody of, assets protectively marked up to CONFIDENTIAL.

Baseline Personnel Security Standard is carried out within the Authority as part of the recruitment process. The Baseline Personnel Security Standard comprises verification of four main elements:

- Identity
- Employment history
- Nationality and immigration status
- Unspent criminal record

Procedure for the Verification of Unspent Criminal Records

Basic Disclosure

Verification of unspent criminal records will be undertaken in the form of a basic disclosure. A basic disclosure is a document containing impartial and confidential criminal history information held by the police and government departments which can be used by employers to make safer recruitment decisions.

Cost

The Authority will cover the cost of a basic disclosure required for all Authority staff and prospective employees.

Basic Disclosure Application Form

The basic disclosure application form and guidance notes are available from the Resourcing team, People and Organisational Development Department (POD).

Supporting Documents

Applicants will be required to show two documents to verify their identity and current address to the Resourcing Team, POD on submission of a basic disclosure application form. These could be:

- A passport, driving licence or birth certificate which shows your date of birth (photographic ID is preferred)
- A utility bill, bank, mortgage or credit card statement that shows your address and should be dated within the last 3 months.

Please note that copies of these documents will be posted with the paper application form, to Disclosure Scotland.

Requests for Further Information

Whilst processing the application, Disclosure Scotland may contact the applicant if further information is required. This information must be provided promptly. Any delay in providing this information may result in the withdrawal of any conditional offer of employment.

Receiving the Disclosure Information

The final disclosure certificate following the application process can be sent direct to either the applicant's home address or the Authority, from Disclosure Scotland. If the disclosure certificate is sent direct to the Authority, this must be upon the consent of the applicant.

If the applicant chooses to have the disclosure certificate sent direct to their home they will be required to show the Authority their original disclosure certificate upon receipt. The Authority will sight this document and obtain a copy for recruitment purposes.

No offer of employment or start date with the Authority will be confirmed until a satisfactory basic disclosure certificate has been sighted.

Reviewing the Result of the Disclosure

POD will assess the content of the Disclosure. Any information received will be considered in line with the duties of the post to which you have been conditionally offered.

Satisfactory Disclosure

If a disclosure is considered to be satisfactory, the applicant will have met this condition of appointment and will receive no further correspondence from the Authority about this matter.

Disclosure which requires further review

Where the Disclosure confirms details of unspent convictions, this will not lead to an automatic bar from appointment. POD will review the contents of the Disclosure in line with the requirements of the vacancy and will consider any other information which the applicant has provided regarding their case. As part of this review the applicant may be invited to discuss their case further with a POD manager (appropriate managerial representatives from the recruiting department may also be involved) before a final decision on suitability is made.

All aspects of the review of the Disclosure will be in line with the Authority's Policy Statement on **the Recruitment and Employment of Ex-offenders** attached as **Appendix A** and **Equal Opportunities Policy** available on the Authority's internal portal.

If the individual's circumstances are not compatible with the post, the Authority may be required to withdraw the offer of appointment and will inform all appropriate parties of this outcome.

Management of Information

All documentation relating to the Disclosure application process will be considered highly confidential by all parties involved and will be stored securely by POD, separately from your personal file. Access to documents, and the results of the Disclosure, will be restricted to those who require access as part of their duties, as determined by POD. Documents will only be retained for a reasonable period following which they will be destroyed as confidential material in line with DBS guidance.

Further details are available in the Authority's Policy Statement on the **Secure Handling, Use, Storage, Retention and Destruction of Disclosure Information** attached as **Appendix B**.

Aftercare

In order to ensure ongoing assurance of certain sensitive posts individuals may be required to engage in an annual security appraisal with their line manager.

2. Non-Police Personnel Vetting Level Three (NPPV3)

The NPPV3 level police check is required for any individuals who as part of their role or location of work are required to access the Joint Control Centre or any similar location where MFRS is working in partnership with the police.

This is required by the Merseyside Police to maintain a high standard, preserve the integrity of the force, safeguard assets, gain the trust of the public and deter corrupt/inappropriate behaviour.

Procedure

The checks conducted include:

- Police National Computer check (PNC)
- Intelligence databases including special branch
- Voters register
- Vetting database
- Credit reference
- Secured Network Services (SNS)

Cost

There is no financial impact for the employee.

Application form

The application form is available from the Resourcing team, People and Organisational Development (POD)

Requests for further information

Whilst processing the application, Merseyside Police may contact the applicant if further information is required. This information must be provided promptly. At this stage MFRS are not included in the communications between the Police and the individual.

Decision

The result will be provided to the Resourcing Team who will then forward to the applicant. Merseyside Police will then issue an access card. Unless there is an organisational need this process will renew after 10 years.

Adverse NPPV3 decisions & appeals

If the application is rejected, the individual does have the right of appeal. In the first instance the individual should contact **force.vetting.unit@merseyside.pnn.police.uk**. If clearance is denied, individuals will be informed of the reason on request and this will be provided unless the reason:-

- Damages National Security
- Frustrates the prevention/detection of crime
- Results in the disclosure of sensitive information
- Breaches confidentiality of any information provided in confidence
- Impedes the apprehension or prosecution of offenders.
- Results in the force breaking the law

If the individual wishes to appeal, it is the individual's responsibility to make the appeal direct to the Head of Professional Standards, Merseyside Police and the appeal will be heard in 5 working days.

MFRS – Implications of Rejection

In the case of an employee being rejected by Merseyside Police, the implications will be reviewed by a member of the People & Organisational Development Team on a case by case basis.

Management of Information

All documentation relating to the NPPV3 application process will be considered highly confidential by all parties involved and will be stored securely by POD. Once the application is approved the application form will be destroyed as confidential material in line with the **SI 0759 Destruction of Information Assets including protectively marked information.**

3. NATIONAL SECURITY VETTING (NSV)

a. Counter Terrorism Check (CTC)

CTC clearance is required for those individuals who are to be employed in posts which:

- Involve proximity to public figures who are assessed to be at particular risk from terrorist attack;
- Give access to information or material assessed to be of value to terrorists;
- Involve unescorted access to certain military, civil, industrial or commercial establishments assessed to be at risk from terrorist attack.

b. Security Check (SC)

Those who are cleared to SC level may have long-term, frequent and uncontrolled access to SECRET assets, and occasional, supervised access to TOP SECRET assets as defined in the Government Protective Marking System.

A Security Check may also be applied to staff that are in a position directly or indirectly to bring about the same degree of damage as those described above or who need access to protectively marked material originating from other countries or international organisations. A Security Check clearance will normally consist of:

- Check against the National Collection of Criminal Records and relevant service and police records;
- Check against Security Service records;
- Credit reference check and, where appropriate, a review of personal finances.
- In some circumstances, further enquiries, including an interview with the subject, may be carried out.

A Security Check clearance should not usually be required for:

- Occasional access to SECRET assets in the normal course of business or during conferences or courses.
- Custody of a small quantity of SECRET assets.
- Entry to an area where SECRET assets are stored.
- Work in areas where SECRET or TOP SECRET information might be overheard.
- Use of equipment capable of handling SECRET information (provided that access controls are in place).
- In these circumstances, the Baseline Personnel Security Standard should usually be sufficient.

c. Developed Vetting (DV)

Those who are cleared to DV level may have long term, frequent and uncontrolled access to TOP SECRET information or assets as defined in the Government Protective Marking System.

This level of clearance may also be applied to people who are in a position directly or indirectly to cause the same degree of damage as those described above and in order to satisfy the requirements for access to protectively marked material originating from other countries and international organisations. In addition to a Security Check, a Developed Vetted will involve:

- An interview with the person being vetted;
- References from people who are familiar with the person's character in both the home and work environment. These may be followed up by interviews.

Enquiries will not necessary be confined to past and present employers and nominated character referees.

NSV Procedure (a, b and c above)

Stage 1

If after a thorough risk assessment a post is deemed as requiring a level of NSV a formal request from the post holders line manager detailing the reasons for this request must be sent to **Contracts&PolicyTeam@merseyfire.gov.uk.** Subsequently, The Department for Communities & Local Government (DCLG) will be contacted to commence the vetting process.
DCLG is the Government Sector Sponsor Department for providing National Security Vetting for the all Fire & Rescue Services, where the requirement for NSV is demonstrable.

Stage 2

The applicant will receive an email direct to their work email address containing guidance sent from the DCLG vetting team. Applicants must read the guidance and complete all relevant parts of the Application for National Security Vetting Clearance form titled 'Annex A'.

The form will request the details of the 'Candidate HR contact details' which the applicant should detail as **Contracts&PolicyTeam@merseyfire.gov.uk**.

Once complete, 'Annex A' should be sent under confidential cover, including wet signatures, to the Vetting Team within POD who will then forward to DCLG by recorded delivery. The applicant must keep a copy of this document for their records and to assist the log in process in stage 3.

If any section of the form is incomplete, the form will not be processed and the sender notified accordingly.

Please note, there are strict deadlines in which stages of the application process have to be completed by. Applicants must adhere to these deadlines. Failure to adhere to these deadlines will have a costly monetary impact for DCLG and may therefore result in a complaint being submitted to the Chief Fire Officer may result in disciplinary action being taken against the applicant as per the Authority's Disciplinary procedure.

Stage 3

If NSV is granted, the Defence Business Services will be notified, who will email the applicant the necessary access to the Cerberus vetting system.

The Vetting Team within POD will also be contacted at this point for further information on the applicant. At this point, the applicant may be requested to provide their original passport to a member of the Vetting Team within POD.

The Defence Business Services and the sponsoring government department will then take responsibility for the remainder of the vetting process.

Duration of application

The duration of a NSV application is dependent on the level of clearance requested and the level of inquiry particular to each application. The length of time between receipt of application and decision on security clearance ranges from 3 weeks to 3 months. The applicant will be notified direct of the outcome in respect of the security clearance decision.

Decision

The decision to grant or decline clearance will be taken by a Government Departmental Security Officer, in collaboration with the Chief Fire & Rescue Adviser (CFRA) Senior Fire & Rescue Security Adviser where necessary. However, before making a final decision, the Departmental Security Officer and/or CFRA Senior Fire & Rescue Security Adviser may ask for additional checks or enquiries to be made, calling the applicant for an interview, or asking for additional referees.

If the subject absolutely refuses to discuss a relevant matter it will be necessary to point out that the Authority will have no alternative but to take this into account in reaching a decision and this might, ultimately, lead to refusal of a new clearance or the removal of an existing clearance.

Circumstance which may present a risk to security

These factors may justify a decision to refuse, limit or withdraw vetting clearance. The list should not be considered exhaustive:

- Significant financial difficulties or debts.
- Compulsive drinking or gambling.
- Illegal use of controlled or prescribed drugs.
- Other conduct likely to lead to such pressure.
- The likelihood that the applicant's performance of duty will be adversely affected e.g. through adverse pressure or a conflict of interest.
- The nature, number and seriousness of any recorded offences or involvement in criminal activity and the time period within which these took place.
- If the circumstances are likely to bring discredit to the Authority or cause embarrassment.
- If the fact of any conviction will genuinely induce a conflict of interest in the discharge of the applicant's duties.

Commencement of work prior to receipt of NSV

Where there is to be a change in personnel filling a vettable post, it is important to ensure that, as far as is practicable, the new incumbent is cleared before taking up post. Where that is not possible the process should be put underway at the earliest opportunity. In the interim, every effort should be made to ensure that the individual does not have access to material for which they have not been cleared.

Change of circumstances

It is a statutory requirement and an individual's responsibility to report any relevant changes to their circumstances that may impact on the suitability to hold a security clearance to their line manager. This is especially important for those individuals whose roles require NSV at CTC, SC and DV levels.

It is the responsibility of line managers to ensure that the Vetting Team within POD is notified of relevant changes coming to their attention.

Failure to notify your line manager of any changes which might affect security clearance may be subject to disciplinary action as per the Authority's Disciplinary procedure.

Aftercare

Personnel Security controls are based on a 'snapshot in time' and an individual's personal circumstances may be subject to a significant change which may affect their suitability to maintain their clearance.

It is therefore vital that the individual's suitability is assessed through an aftercare regime. This may require checks to be carried out to determine whether the changes represent a potential risk to the integrity of the Authority.

Staff subject to NSV will be contacted by the Vetting Team within POD on an annual basis to undertake a security appraisal. This routine but important process is required for all individuals

cleared to the highest levels in order to review the continued suitability to access highly classified information and assets. The appraisal allows the Authority to update records to reflect any changes to personal circumstance and identify and review any issues that may relate to security

The Authority may need to make follow-up enquiries concerning information provided, particularly where personal circumstances have changed.

Renewal of NSV clearance

A clearance does not last indefinitely therefore individuals whose clearance is due for renewal will be required to complete new questionnaires. The process will be conducted in line with the criteria for initial vetting. Any level of clearance may be renewed at an earlier stage if a higher clearance is required or reviewed if information comes to light relating such as a material change in an employee's personal circumstances.

Leaving a post requiring NSV

Once an individual has left a vettable post, making the clearance requirement redundant, the applicant must advise the Vetting Team within POD who will in turn advise DCLG of this change.

In cases when staff end their employment, their vetting clearance will be revoked. Where they are required to resign as an alternative to dismissal, or are dismissed from the Authority, or resign prior to misconduct hearing, where there are clear concerns about their integrity or ability to hold NSV clearances, the Security Service will be notified immediately.

Adverse NSV decisions & appeals

The appeals procedure for NSV is available to those individuals refused NSV clearance.

Where a National Security Vetting clearance request is refused, or where withdrawal of National Security Vetting clearance has taken place, a process exists that requires an appeal to DCLG. The appeal may result in the original decision to refuse or withdraw clearance being overturned.

Request for an appeal or review must be made in writing, and must be from the applicant themselves, or endorsed by the applicant. The appeal should then be submitted to the DCLG Departmental Security Officer within 10 working days of receiving notification of the refusal/withdrawal.

MFRS – Implications of Rejection

In the case of an employee being rejected following the NSV process, the implications will be reviewed by a member of the People & Organisational Development Team on a case by case basis.

Career breaks & secondments

Individuals on career break or secondment will continue to be regarded as employees of the Authority and remain subject to the Authority's conditions of service.

All individuals who have been on career break or secondment may be required to submit a full vetting application and must provide written declaration indicating whether or not they have come to the attention of the police or relevant Law Enforcement Agencies, through their POD contact prior to their return. The application will be clearly marked indicating the length of time the employee has been on career break or secondment together with the details of any time spent out of the Country.

Retention of NSV records

All papers obtained during the course of the vetting enquiries and utilised in the decision making process, whether clearance is granted or not, will be retained for the period shown below:

- If cleared the papers will be retained for the duration of the clearance.
- 1 year after leaving the Authority.
- 1 year after any vetting clearance is withdrawn.
- 3 years after any vetting clearance is refused.

APPENDIX A

"An Excellent Authority"

POLICY ON THE RECRUITMENT OF EX-OFFENDERS

Policy Statement

1. The Code of Practice ("the Code") is published by the Secretary of State under section 122 of Part V of The Police Act 1997 ("the 1997 Act"). The Code identifies obligations which registered bodies, counter signatories and other recipients of disclosure information issued under the 1997 Act and the Safeguarding of Vulnerable Groups Act ("the 2006 Act").
2. We comply with the Code, the 1997 and 2006 Acts regarding the treatment of individuals who are subject to Disclosure Scotland checks. We undertake not to discriminate unfairly against the subject of a disclosure on the basis of conviction or other information revealed.
3. We will provide a copy of this policy and the Code to anyone who asks to see it.
4. We are committed to equality of opportunity, to following practices, and to providing a service which is free from unfair and unlawful discrimination. We ensure that no applicant or member of staff is subject to less favourable treatment on the grounds of offending background. We actively promote the right mix of talent, skills and potential and welcome applications from a wide range of candidates, including those with criminal records. The selection of candidates for interview will be based on skills, qualifications and experience.
5. We will use a Disclosure Scotland check only where this is considered proportionate and relevant to the particular position or type of regulated work. This will be based on a thorough risk assessment of the position or work and having considered the relevant legislation which determines whether or not a Standard or Enhanced Disclosure under the 1997 Act or a request for disclosure under the 2006 Act is applicable.
6. Where a disclosure application or request is deemed necessary, individuals will be made aware that the position or work will be subject to a Disclosure Scotland check and that the nature of the position or work entitles us to ask about spent and unspent convictions.
7. We will ask individuals to complete a criminal record self-declaration form. We will stress to individuals that they should be honest in their response. We will ask that this form be returned under separate, confidential cover, to a designated person within our organisation and we guarantee that this form will only be seen by those who need to see it as part of the decision-making process.
8. At interview, or under separate discussion, we undertake to ensure an open and measured discussion on the subject of any offences or other matters that might be considered relevant for the position or work concerned.
9. We undertake to discuss any matter revealed in a certificate issued under the 1997 Act or a Scheme Record issued under the 2006 Act with the subject of that disclosure before a decision is made.
10. We ensure that all those who are involved in the decision making process have been suitably trained to identify and assess the relevance and circumstances of disclosure information. We also ensure that they have received appropriate guidance and training about providing work for ex-offenders.

HAVING A CRIMINAL RECORD WILL NOT NECESSARILY DEBAR YOU FROM WORKING WITH US.

1 We are only able to discuss what is contained on a Disclosure Certificate and not what may have been sent under separate cover by a police force.

APPENDIX B

"An Excellent Authority"

POLICY ON THE SECURE HANDLING, USE, STORAGE, RETENTION AND DESTRUCTION OF DISCLOSURE INFORMATION

Note: The Authority has several service instructions relating to information security and governance that may also be relevant. However, in the case of basic disclosure information the process in this appendix must also be followed.

Policy Statement

Introduction

1. The Code of Practice ("the Code") is published by the Secretary of State under section 122 of Part V of The Police Act 1997 ("the 1997 Act"). The Code sets out obligations for registered bodies, counter signatories and other recipients of disclosure information issued under the 1997 Act and the Safeguarding of Vulnerable Groups Act 2006 ("the 2006 Act").

General Principles

2. We comply with the Code and the 1997 and 2006 Acts regarding the handling, holding, storage, destruction and retention of disclosure information provided by Disclosure Scotland. We comply with the Data Protection Act 1998 ("the 1998 Act"). We will provide a copy of this policy to anyone who requests to see it.

Usage

3. We will use disclosure information only for the purpose for which it was requested and provided. Disclosure information will not be used or disclosed in a manner incompatible with that purpose. We will not share disclosure information with a third party unless the subject has given their written consent and has been made aware of the purpose of the sharing.

Handling

4. We recognise that, under section 124 of the 1997 Act it is a criminal offence to disclose disclosure information to any unauthorised person. Disclosure information is only shared with those authorised to see it in the course of their duties. We will not disclose information provided under subsection 113B(5)2 of the 1997 Act, namely information which is not included in the certificate, to the subject.

Access and Storage

5. We do not keep disclosure information on an individual's personnel file. It is kept securely, in lockable, non-portable storage containers. Access to storage units is strictly controlled and is limited to authorised named individuals, who are entitled to see such information in the course of their duties.

Retention

6. To comply with the 1998 Act, we do not keep disclosure information for longer than necessary. For the 1997 Act, this will be the date the relevant decision has been taken, allowing for the resolution of any disputes or complaints. For the 2006 Act, this will be the date an individual ceases to do regulated work for this organisation. We will not retain any paper or electronic image of the disclosure information. We will, however, record the date of issue, the individual's name, the disclosure type and the purpose for which it was requested, the unique reference number of the disclosure and details of our decision. The same conditions relating to secure storage and access apply irrespective of the period of retention.

Disposal

7. We will ensure that disclosure information is destroyed in a secure manner i.e. by shredding, pulping or burning. We will ensure that disclosure information which is awaiting destruction will not be kept in any insecure receptacle (e.g. a waste bin or unlocked desk/cabinet).

Umbrella Bodies

8. Before acting as an Umbrella Body (a body which countersigns applications for Standard or Enhanced Disclosures or makes declarations in relation to PVG disclosure requests on behalf of other organisations) we will take the following steps. We will ensure that the organisation on whose behalf we are acting complies with the Code and the 1997 and 2006 Acts. We will take all reasonable steps to satisfy ourselves that they will handle, use, store, retain and dispose of disclosure information in full accordance with this policy. We will also ensure that anybody or individual for whom applications or requests are countersigned, has such a written policy. If necessary, we will provide a model policy for that body or individual to use or adapt for this purpose.

This page is intentionally left blank

Merseyside Fire and Rescue Service

Equality Impact Assessment Form

Title of policy/report/project:	**Protective Security including:** **Protective Security Policy** **Protective Marking SI** **Personnel Security SI**
Department:	**Strategy and Performance**
Date:	**10/1/14**

1: What is the aim or purpose of the policy/report/project

This should identify "the legitimate aim" of the policy/report/project (there may be more than one)

Protective Security is the term used to describe the actions/policies required to meet the threats to an organisation and to protect its assets from compromise. Protective Security is important when considering the political climate and the technology that poses threats and risks to the Fire and Rescue Service. Effective security is important in maintaining the confidence of the public, staff, stakeholders and partner agencies in efficient, effective and safe service delivery. Protective Security is a holistic process that covers three related aspects of security; information (documents/data systems), personnel (staff/customers) and physical (buildings/estates/property).

The Authority's aim is to achieve compliance, as far as practicable, with the relevant aspects of HMG Security Policy Framework, and as detailed within the DCLG Fire & Rescue Protective Security Strategy. To this end, a working group has been set up to implement the requirements of the Fire and Rescue Service Protective Security Strategy. A draft policy and two service instructions have been developed.

2: Who will be affected by the policy/report/project?

This should identify the persons/organisations who may need to be consulted about the policy /report/project and its outcomes (There may be more than one)

Staff (including contractors, partners, volunteers)
Authority Members
Visitors to FRS premises

The Service Instructions that will be used to deliver against the policy will be

developed over time and this EIA will be reviewed and amended as each one is developed.

3. Monitoring *Summarise the findings of any monitoring data you have considered regarding this policy/report/project. This could include data which shows whether the it is having the desired outcomes and also its impact on members of different equality groups.*	
What monitoring data have you considered? No monitoring data is available in relation to the policy and Service Instructions from an equalities perspective. This will be collected as the policy and SIs are implemented. This EIA will then be reviewed and updated accordingly.	**What did it show?**

4: Research *Summarise the findings of any research you have considered regarding this policy/report/project. This could include quantitative data and qualitative information; anything you have obtained from other sources e.g. CFOA/CLG guidance, other FRSs, etc*	
What research have you considered? The FRS Protective Security strategy Protective Security implementation documents from other FRS Protective Security implemention documentation from non-FRS organisations	**What did it show?** There are a number of actions required to ensure compliance with the three aspects for Protective Security. These include implementing protective marking, implementing staff security checks and reviewing and (if appropriate) improving physical security, including building security. The Personnel Security SI will have an impact on staff, contractors and volunteers, as new security checks (Baseline Personnel Security Standard) will be required, initially for some, but eventualy for all staff, contractors and volunteers. These checks are not considered particularly intrusive but involve criminal records checks

	to replace the individual applying for a job providing that information as was previously the case. Existing staff are already required to inform the organisation if they receive a criminal conviction whilst in employment. In the future all staff, volunteers and contractors will be the subject of the same check as that used at recruitment. The decision on who requires a check and when they require it will be taken based on the risks associated with the information and other organisational assets they have access to, but over time all staff will be receive a BPSS check.

5. Consultation

Summarise the opinions of any consultation. Who was consulted and how? (This should include reference to people and organisations identified in section 2 above) Outline any plans to inform consultees of the results of the consultation

What Consultation have you undertaken?	**What did it say?**
Discussions within the Protective Security working group	A range of staff covering several departments considered the potential implications of the policy and SIs. Full implementation of Protective Security will result in tighter control of access to information and other assets and staff, contractors and volunteers will feel some impact from this in relation to personnel security checks. One consideration identified is the issue of what action would be taken if a security check highlighted convictions that an employee had not informed MFRA about. This could have equality and diversity implications, (ie in the way decisions are then made about individuals) and this is under consideration. However, it is accepted that the FRS Protective Security Strategy should be implemented to protect the assets MFRA is responsible for and protect staff. Future developments could include implications for staff, contractors and the public when physical (including building) security is reviewed and this is likely to have an impact on access to MFRA buildings. EIA implications will be considered as the work continues.
Related discussions between POD and Joint secretaries on a Police vetting system	MFRA has been consulting with Joint secretaries on the introduction of Police Vetting for some staff in relation to access to the Joint command and Control Centre. Although it is not directly related to Protective Security

	and the BPSS checks, there are some connections and POD will introduce the BPSS into its discussions with Joint Secretaries.
Policy and Service Instruction consultation process	The Policy, Protective Marking SI and Personnel Scurity SI have all been through the 21 day consultation period with no comments received.

6. Conclusions

Taking into account the results of the monitoring, research and consultation, set out how the policy/report/project impacts or could impact on people from the following protected groups? (Include positive and/or negative impacts)

(a) Age

The implications of the Policy and SI are currently considered to be neutral in relation to this protected group.

(b) Disability including mental, physical and sensory conditions)

The implications of the Policy and SI are currently considered to be neutral in relation to this protected group.

(c) Race (include: nationality, national or ethnic origin and/or colour)

The implications of the Policy and SI are currently considered to be neutral in relation to this protected group.

(d) Religion or Belief

The implications of the Policy and SI are currently considered to be neutral in relation to this protected group.

(e) Sex (include gender reassignment, marriage or civil partnership and pregnancy or maternity)

The implications of the Policy and SI are currently considered to be neutral in relation to this protected group.

(f) Sexual Orientation

The implications of the Policy and SI are currently considered to be neutral in relation to this protected group.

(g) Socio-economic disadvantage

The implications of the Policy and SI are currently considered to be neutral in relation

to this protected group.

7. Decisions

If the policy/report/project will have a negative impact on members of one or more of the protected groups, explain how it will change or why it is to continue in the same way.
If no changes are proposed, the policy/report/project needs to be objectively justified as being an appropriate and necessary means of achieving the legitimate aim set out in 1 above.

This EIA will remain under review as the policy and SIs are implemented.

- MFRA will put in place arrangements to make sure that where someone "fails" a check (ie criminal convictions are identified) that this will be dealt with in an in an equitable way for all staff.

- MFRA will monitor the results of the personnel security arrangements 12 months after commencement with the Diversity and Consutaltion Manager

8. Equality Improvement Plan

List any changes to our policies or procedures that need to be included in the Equality Action Plan/Service Plan.

9. Equality & Diversity Sign Off
The completed EIA form must be signed off by the Diversity Manager before it is submitted to Strategic Management Group or Authority.

Signed off by: Wendy Kenyon **Date:** 21.1.2014

Action Planned	Responsibility of	Completed by
Monitor the results of the personnel security arrangements and the arrangements being used when someone "fails " the security checks	Director of S and P , POD and Diveristy and Consutaltion Manager	Jan 2015

For any advice, support or guidance about completing this form please contact the DiversityTeam@merseyfire.gov.uk or on 0151 296 4237

The completed form along with the related policy/report/project document should be emailed to the Diversity Team at: DiversityTeam@merseyfire.gov.uk

MERSEYSIDE FIRE AND RESCUE AUTHORITY			
MEETING OF THE:	**POLICY AND RESOURCES COMMITTEE**		
DATE:	**1 APRIL 2014**	**REPORT NO:**	**CFO/039/14**
PRESENTING OFFICER	**DEPUTY CHIEF FIRE OFFICER**		
RESPONSIBLE OFFICER:	**DEB APPLETON**	**REPORT AUTHOR:**	**DEB APPLETON**
OFFICERS CONSULTED:	**SUE NASH, PROJECT MANAGEMENT OFFICER**		
TITLE OF REPORT:	**REVIEW OF IMPROVEMENT SCHEME**		

APPENDICES:	

Purpose of Report

1. To inform Policy and Resources Committee of progress and outcomes in relation to the Authority's Improvement Scheme.

Recommendation

2. That Members note the progress and outcomes resulting from the Improvement Scheme.

Introduction and Background

3. Members will recall that the Improvement Scheme was implemented in December 2012 to replace the IDEAS Scheme which had run for several years; initially successfully, but latterly with fewer good quality suggestions being advanced. The IDEAS scheme rewarded successful suggestions with a payment to the staff member concerned, although any suggestions could not be in relation to the employees own work area. In contrast, the Improvement Scheme offers opportunities for tailored development or involvement in an implementation project rather than a cash reward, and suggestions can be related to an individual's work area.

4. The Improvement Scheme was launched in December 2012 with a dedicated section of the Portal set up to receive applications and announcements made to staff that the scheme was in operation. Approximately two suggestions per month have been submitted to the Improvement Scheme since the change in approach.

5. Of the 28 suggestions received, not all contained sufficient information to make a decision whether to implement and although further information has been

requested, this has not always been provided. Five suggestions have been approved and are in various stages of implementation as outlined below:

1. **To procure hi viz signs/tape to assist manoeuvring of appliances at Kirkdale station – Submitted by a Watch Manager**

   This was considered a straight forward solution to a known problem at this location and the high visibility tape was procured.

2. **Picture book intervention - book for information and intervention with young people: - Submitted by a firefighter**

   This suggestion was submitted by the author of the book and following provisional agreement a short feasibility study was carried out. It was agreed that there was some merit in supporting this suggestion but work to produce teaching notes is ongoing and issues of intellectual property rights are still being considered.

3. **On-line equipment swap – Submitted by a firefighter**

   This suggestion related to ensuring that any operational equipment swapped between crews at operational incidents is easily located and returned to its original appliance/station through an on-line solution. The suggestion was taken forward by Appliances and Equipment department as part of their overall review of all internal and incident ground logistics. This review includes the whole equipment recovery and repatriation procedure.

4. **Delivering RTC reduction engagement with employers that employ young people – Submitted by a firefighter**

   The suggestion was that the Service could reach more young people at higher risk of being involved in a road traffic collision by targeting particular employers that employ a higher number of young people. In addition, those in employment are more likely to own a car. The applicant was invited to work with the Prevention and Protection road traffic collision reduction team to develop this idea further.

5. **Displaying open HFSC appointments on the fire appliance Mobile Data Terminal (MCT) – Submitted by a firefighter**

   This suggestion involved adding details of homes requiring a Home Fire Safety Check (HFSC) to the MDTs so crews could make more effective use of their time when in the community and could reduce the need for extra journeys to be made to complete HFSCs. It was agreed that the idea has the possibility of being expanded to include all to the HFSC Status Reports, which display unvisited properties in order of risk. The suggestion has been taken forward by Strategy and Performance, Prevention and Protection and ICT departments and although currently it is not possible to do this, it will be when MDTs are upgraded.

6. Members will see from the information above that a number of suggestions have been successful and that they represent engagement with firefighters and cover a number of areas of service delivery. For this reason it is considered a useful scheme to retain. As there has been a lull in submissions so far in 2014 it is intended to remind staff about the scheme and to promote it through the Portal and Hot News in In order to encourage more staff to make suggestions to improve the workplace and the services provided by MFRS.

Equality and Diversity Implications

7. It should be noted that of the 28 suggestions received 25 were from men and 3 from women. 26 were from uniformed staff and 2 from non-uniformed. Of the five successful suggestions, all were from male uniformed staff. Consideration will be given to encouraging more women and non-uniformed members of staff to participate.

Staff Implications

8. There are no staff implications arising from this report.

Legal Implications

9. There are no legal implications arising directly from this report. Any legal issues arising from individual suggestions are raised with the legal department.

Financial Implications & Value for Money

10. There are no financial implications arising from this report.

Risk Management, Health & Safety, and Environmental Implications

11. Several suggestions relate to various types of risk and/or health and safety improvements.

Contribution to Our Mission: *Safer Stronger Communities – Safe Effective Firefighters*

12. Staff making suggestions about how to improve the working environment and services provided by MFRS is beneficial to our communities.

BACKGROUND PAPERS

CFO/111/11 If this report follows on from another, list the previous report(s)

GLOSSARY OF TERMS

This page is intentionally left blank

This report is Restricted

This page is intentionally left blank

This report is Restricted

This page is intentionally left blank

This report is Restricted

This page is intentionally left blank