Strategic Planning, Performance and Communications

SCOTTISH FIRE AND RESCUE SERVICE
Working together for a safer Scotland

INFORMATION GOVERNANCE

INFORMATION SECURITY HANDBOOK

Author/Role	Lynne McAlonan, Information Security Officer
Date of Risk Assessment (if applicable)	N/A
Date of Equality Impact Assessment	In progress
Date of Impact Assessment (commenced)	N/A
Date of Impact Assessment (concluded)	N/A
Quality Control (name)	Carol Wade, Information Governance Manager
Authorised (name and date)	DACO Alasdair Perry – 26 September 2017
Last reviewed/amended (name and date)	Lynne McAlonan – April 2019 section 3.7 amended
Date for Next Review	October 2020

STRATEGIC PLANNING, PERFORMANCE AND COMMUNICATIONS

INFORMATION GOVERNANCE

INFORMATION SECURITY HANDBOOK

1. INTRODUCTION

Information Governance is committed to safeguarding the Scottish Fire and Rescue (SFRS) information from unauthorised access, disclosure or modification to ensure its:

- Confidentiality (assurance that information is not made available or disclosed to unauthorised individuals, entities, or processes);
- Integrity (assurance that information is not accidentally or maliciously altered or destroyed);
- Availability (assurance that authorised users have access to information resources when required).

We ensure that:

- Information assets (data, system, computer, network device, document or any other component of the Service's infrastructure which stores, processes or transmits data) shall be protected against unauthorised access;
- Confidentiality of information assets shall be a high priority;
- Information shall be protected from unauthorised disclosure;
- Integrity of information shall be maintained;
- Statutory and legal obligations shall be met;
- All breaches of information security, actual or suspected, shall be reported and investigated in line with SFRS published policies;
- Implemented controls shall be commensurate with the risks faced by SFRS.
- Proper record keeping of the source, authority and purpose for personal information shared;

- Use of personal information sharing is consistent with the purpose stated at the time of collection;

- Appropriate information handling procedures are established and complied with.

2. PURPOSE

This handbook provides staff with a guide to Information Security within the SFRS, relevant associated policies and the expectations of the Service.

3. ACCEPTABLE USE

SFRS must ensure that employees understand the way in which ICT, including electronic mail (email), the Internet, Communications, voicemail, telephony and other computer equipment and services, should be used within the Service (this list is not exhaustive). It aims to ensure that ICT is used effectively for its intended business purpose without infringing legal requirements or creating unnecessary business and corporate risk. Standards are set for using ICT equipment throughout the Service and equally when accessing SFRS systems remotely where authorised. The following activities are expressly forbidden:

- The introduction of any form of computer virus;

- Seeking to gain access to restricted areas of the network or other hacking activities;

- Forgery or attempts to read other users' mail without their or SFRS express permission.

- Unauthorised access or attempts to access any administrative account on any SFRS ICT systems;

- Removal of any hardware, software or files without authorisation;

- Installation or attempts to install hardware or software without authorisation;

- Connecting or attempting to connect privately owned computer hardware to any part of the SFRS network without the explicit consent of the Head of ICT;

- The removal of any mobile devices, such as laptops and tablet devices, from SFRS premises without the prior consent of the Head of ICT. All mobile devices must be password protected and, if they are to be used off-premises, they should be in view of the responsible staff member at all times and never left unattended.

3.1 Confidentiality

All information relating to the business operation of SFRS is confidential. Employees are expected to treat electronic information with the same care as confidential paper-based information. All information must be kept secure and used only for its intended purpose.

Users' passwords are to be kept secure, they must comply with the SFRS Network Password Policy and must not be disclosed to anyone.

Users must return any e-mail message received that was intended for another recipient and then delete any copies of misdirected messages.

3.2 Use of E-Mail

E-mails sent from the Service have the same weight in law as though they were sent to the recipient on headed notepaper. Care should therefore be taken when composing e-mails to avoid:

- Creating unintended contractual agreements through acceptance or acknowledgement of another party's offer or conditions;

- Distributing unlawful, offensive or inappropriate material for which the Service would be held responsible and could be prosecuted;

- Transmission of unsolicited, commercial or advertising material, chain letters or junk mail of any kind;

- Unauthorised transmission to a third party of sensitive information concerning the activities of SFRS. Unencrypted e-mails sent outside the Service can be easily intercepted and read by someone with basic equipment and technical knowledge. Information which is protectively marked should not be sent by e-mail unless using a 'secure email account licence'. The secure email software used by SFRS is Egress Switch;

- Transmission of material such that this infringes the copyright of another person, including intellectual property rights;

- Activities that waste staff effort or networked resources or activities that deny service to others, e.g. sending large attachments to numerous recipients;

- Transmission of obscene, offensive or indecent images or data;

- Creation or transmission of material that discriminates or encourages discrimination on social, ethnic, gender, sexual orientation, marital status, disability and religious or political beliefs;

- Creation or transmission of defamatory material that includes claims of a deceptive nature;

- Criticising individuals, including copy distribution to other individuals;

- Publishing to others the text of messages written in confidence without express consent of the author;

- Transmission of any message that could bring SFRS into disrepute.

Remember that what might seem like a harmless comment in a face to face situation may appear to be offensive in an e-mail, since the recipient has no eye contact with which to judge the tone of the comment.

- Personnel should consider if using the phone is a more appropriate means of communication;

- Emails are not confidential and can be read by anyone given a degree of expertise;

- Emails should be regarded as published material.

Email messages and other files that have been deleted from ICT systems can be traced and retrieved. Therefore, all persons having a part in creating or forwarding any offending email or file can be identified. Emails and computer records, both in hard copy and electronic form, are admissible in a court of law.

3.3 Use of Internet

SFRS provides Internet access for business purposes only. However, occasional personal use of the Internet facility will be permitted, provided that it is not abused and complies with other rules in the policy.

You must not access, browse, create, upload or download unlawful or offensive material. Specifically, you must not:

- Knowingly violate any laws or regulations. SFRS will co-operate with any legitimate law enforcement agency in bringing people to justice;

- Knowingly download or distribute software or data;

- Deliberately introduce or pass on any virus or other type of malicious code;

- Download entertainment software or games or play against opponents across the Internet;

- Download images or videos unless there is a specific business related use for the material;

- Download audio files such as MP3, WAV, OGG, etc. unless for business use.

All software MUST be installed by the SFRS ICT Service Desk who implement a process to ensure SFRS have adequate licencing for it.

3.4 Use of Mobile / Portable Media Equipment

Users of mobile equipment, such as laptops, tablets or mobiles, are responsible for their security and ensuring the security of any data held thereon:

- Take steps to avoid being seen by others when, for example, stowing equipment in the car boot. Thieves often wait around motorway service areas watching for equipment being stowed in the boots of cars;
- Ensure portable equipment is stored securely;
- Information held on portable devices must be encrypted. Where equipment holds sensitive data, it should not be left unattended at any time;
- Always use security features provided including password protection;
- Report any loss of mobile equipment immediately to the Information Governance Team and the SFRS ICT Service Desk;
- Command and Control Centres are prohibited from using any Portable Media Devices.

3.5 Use of Microsoft Lync Instant Messages

The Microsoft Lync 2013 system is designed to facilitate business communication and the sharing of corporate information and enables SFRS staff to communicate directly with each other and potentially third parties using Instant Messaging, voice and video conferencing and desktop and screen sharing facilities.

The use of Instant messages sent using the Lync system needs to be carried out with similar precautions to that of creating and sending emails and care should

therefore be taken when composing Instant Messages to avoid:

- Creating unintended contractual agreements through acceptance or acknowledgement of another party's offer or conditions;
- Distributing unlawful, offensive or inappropriate material for which the Service would be held responsible and could be prosecuted;
- Transmission of unsolicited, commercial or advertising material or chain letters of any kind;
- Unauthorised transmission to a third party of sensitive information concerning the activities of SFRS. Lync does not have an inbuilt protective marking facility, therefore Instant Messaging should only be used for content that is Not Protectively Marked;
- Transmission of material such that this infringes the copyright of another person, including intellectual property rights;
- Activities that waste staff effort or networked resources or activities that deny service to others, e.g. sending large attachments to numerous recipients;
- Transmission of obscene, offensive or indecent images or data;
- Creation or transmission of material that discriminates or encourages discrimination on social, ethnic, gender, sexual orientation, marital status, disability and religious or political beliefs;
- Creation or transmission of defamatory material that includes claims of a deceptive nature;
- Criticising individuals, including copy distribution to other individuals;
- Transmission of any message that could bring SFRS into disrepute.

Remember that what might seem like a harmless comment in a face to face situation may appear to be offensive in an Instant Message, since the recipient has no eye contact with which to judge the tone of the comment.

- Personnel should consider if using the phone is a more appropriate means of communication;

- Instant Messages should be regarded as published material.

3.6 Copyright

Copyright laws apply not only to downloaded, copied or transmitted documents but also to software. All SFRS staff must be aware that only the owner of the copyright is allowed to copy the information. This means that information must not be copied without the permission of the copyright owner. If in doubt, staff must seek advice and approval from the copyright owner.

3.7 Printing

- Where pull printing is available in SFRS, this is a secure method of printing. It is a unique way of printing where print jobs are not triggered directly but are temporarily stored on a central print server. Only when the user is at a device of their choice and authenticates at that device does the output of the print job start. SFRS method of authentication at printers is personal reference numbers to each employee; if you key this authentication incorrectly and another user name is displayed, you must log out and input the correct details. Employees must not print any documentation that is not linked their own authentication via the pull printing facility. Non-compliance with this provision shall be investigated in accordance with SFRS Code of Conduct and thereafter reserve the right to invoke the Disciplinary Policy;

- Where pull printing is not available, users are responsible to secure their print jobs;

- Any printout found lying on a device should be handed over to the owner. If the owner is unknown, it should be disposed of and placed in the confidential waste and not left on the device;

- If a device runs out of paper or jams while releasing a print or copy job, ensure that paper is reloaded or jam is cleared to complete the job. If this is not done by the user and later reloaded or cleared by another user, the rest of the print/copy job will be printed and visible to others which poses a risk of disclosing confidential information;

- Preferred communication and storage methods are electronic, print only when necessary and in line with local operating procedures;

- Use colour only when necessary. Colour printing is ten times (10x) more expensive than mono;

- All usage of the devices can be audited. Staff are expected to refrain from using the devices for production of personal materials.

3.8 Good Security Practice

- Passwords must be kept safe and not divulged to anyone else either inside or outside the Service. Do not use passwords that can be easily guessed, such as your child or partner's name. Use strong passwords that include a mixture of upper and lower case, special characters and numbers. If you need further advice on how to do this, contact the SFRS ICT Service Desk or refer to the SFRS Network Password Policy;

- Work-stations (including laptops) will be set up to provide users with appropriate levels of access. Do not access or attempt to access parts of the system that would require additional access rights. Never attempt to gain access to a system by using another person's User ID and Password;

- Always lock your work-station when leaving your desk. You can do this by pressing Ctrl, Alt and Return or Windows L shortcut;

- The Information Systems are protected against viruses and other malware attacks by a comprehensive set of tools that are routinely maintained. You must not interfere with these tools, for example by attempting to disable the anti-virus software on your desktop;

- Information arriving into the Service through the gateways (either by Internet or e-mail) is routinely scanned to ensure that it is free from viruses and malware. All removable media including CD, DVD, USB data sticks containing information to be transferred to the network must be scanned before attempting to connect to the network;

- Any stand-alone equipment not routinely connected to the network will not be protected against virus attack. You must make alternative arrangements to protect any information contained thereon by contacting the SFRS ICT Service Desk;

- Where laptops, tablets or mobiles are being used outside the Service to connect to wireless hotspots at airports, etc. then special care must be taken to ensure viruses are not imported through these connections. Important or sensitive information should not be transmitted through wireless connections, unless an appropriate level of encryption has been established as part of the connection. If you need further advice on encryption, you should contact the SFRS ICT Service Desk.

3.9 General Principles

SFRS provides computer hardware, software and network connectivity to support the completion of technical and administrative tasks. Domain user accounts or local access accounts are provided for employees on this basis. All installation, modification, transport, troubleshooting or repair may only be carried out by SFRS ICT staff or other persons authorised by the Head of ICT. Under no circumstances should staff other than SFRS ICT staff remove or tamper with computer hardware and/or computer accessories.

SFRS provides an email system and internet access to support its activities and access to these resources is granted to employees on this basis. Emails sent or received on the SFRS email system are not private property; they form part of the administrative records of SFRS. All staff must ensure they regularly check emails and respond where necessary and also ensure they monitor activity on the SFRS Intranet. All staff have an individual responsibility to be wary of suspicious email attachments and links, especially in unsolicited emails. Where staff receive a suspicious email, they should not open the attachment or link but should immediately inform the SFRS ICT Service Desk.

Occasional personal use of the SFRS email system and internet access is permitted, subject to the restrictions contained in this policy. Any personal use of email or the internet is expected to be in the employee's own time and must not interfere with their job responsibilities. SFRS email and internet facilities should not be used to facilitate employees within another job/business which they are associated with.

Personal use of the email system or the internet must not negatively affect the job responsibilities of other employees, have the potential to cause distress/disrupt the system and/or harm the reputation of the SFRS.

Personnel should refrain from forwarding desk phones to mobiles but should use the voicemail services provided by SFRS.

3.10 Monitoring

All SFRS ICT resources, including computers, laptops and tablets, email, voicemail, facsimile and telephony are provided solely for business purposes. At any time and without prior notice, SFRS maintains the right and ability to examine any software programme, hardware device or system and inspect and review data recorded on those systems.

Any information stored on any computer hard drive, computer disk or other storage device found within SFRS premises may be subject to scrutiny by the Head of ICT. This examination assists the SFRS to comply with Service policies and Scottish/UK legislation.

In order to ensure compliance with this policy, SFRS may employ monitoring software to check on the use and content of email and internet usage to ensure that there are no serious breaches of the policy.

SFRS specifically reserves the right for authorised personnel to access, retrieve, read and delete any communication that is created on, received through or sent in the email system, to ensure compliance with all Service policies. All monitoring will be used for legitimate purposes only.

To remind you of the SFRS Acceptable Use Policy, please click here.

4. SECURE DESK

Scottish Fire and Rescue Service (SFRS) operate a secure desk policy. This is aimed principally at protecting sensitive commercial and operational information by ensuring it is locked away when not in use. However, a secure desk policy also encourages efficient working, since time is not wasted looking for mislaid information or reprinting documents that have been lost or damaged through accidents and spills.

The objective is to ensure that all paper and electronic records containing person identifiable information or any other confidential/sensitive information is suitably secured when not in use and is not left visible in work areas whilst unattended for an extended period.

4.1 Definitions

Personal Information

Personal information is information which can identify a person – in which the person is the focus of the information and which links that individual to details which would be regarded as private, e.g. name, private address, home telephone number, National Insurance number, etc.

For example, this could include printed spreadsheets of staff and payroll details or address files.

Sensitive Personal Information

Sensitive personal information is where the personal information contains details such as that person's:

- Physical or mental health condition;
- Sexual life;
- Ethnic origin;
- Religious beliefs;
- Political views;
- Criminal convictions;
- Membership of a trade union.

Corporate and Commercially Sensitive Information

Corporate and commercially sensitive information may, through improper disclosure, cause reduced competitiveness or breach procurement practices. Such information may include building leases, commercial / third party contracts or internal plans.

SFRS will be publishing a Government Security Classification Scheme which provides all employees with the security classification categories and guidance on their application. The policy also provides guidance on the storage and dissemination of documents, data and information relevant to the security classification.

4.2 Protecting Information

Sensitive or confidential information, whether held electronically or on paper, and other valuable resources should be secured appropriately when staff are absent from their workplace and at the end of each working day.

To facilitate this, the following guiding principles have been produced which cover both non-electronic (e.g. manual/paper files) as well as electronic forms of information.

In addition, reference is made to the display of information on the computer, laptop, tablet or mobiles screens as well as to the security of personal property.

- Desks must be cleared at the end of each working day. All efforts must be made to keep this information secure and not readily accessible to non-authorised staff;

- All protectively marked information must be locked away when the room is unoccupied, even if only for a short period. In open plan areas, documents must be locked away when not in use;

- To reduce the risk of a breach of confidentiality and adherence to the Data Protection Act, when disposing of person identifiable information, ensure that it is destroyed securely using approved methods of waste disposal;

- Health & Safety – desks and other work spaces should be sufficiently tidy to allow a comfortable working position to be achieved and permit the Service's cleaning staff to perform their duties.

4.3 Electronic Storage Devices

- For the purposes of this policy, electronic data and equipment will not be treated differently from manual records and equipment, if they contain the same type of confidential, sensitive and/or personal information. Computing and all other equipment containing data will therefore be treated with the same level of security as paper based resources;

- To ensure the security of information held electronically, lock away portable computing devices such as laptops, tablets and mobiles when not in use;

- To ensure the security of information held on mass storage devices, such as CDROM, DVDs or USB drives, lock these away in a secure drawer at the end of the working day;

- USB drives and other such items must be locked away even if they are encrypted.

4.4 Personal Computers, Laptops and Personal Digital Assistants (PDAs)

- Computers and laptops must not be left logged on when unattended. When staff have to leave their desks for any reason, they must lock the computer by using the 'Ctrl, Alt, Del' keys simultaneously or by pressing the 'Windows' key and the letter 'L'. Access to the computer/laptop must be protected by passwords. Tablets and mobiles must be secured with PIN Number/passcode;

- As far as practicable, when sensitive or confidential information is being worked on, the screen must be closed or minimised or the computer locked when unauthorised persons are in close proximity to the screen.

4.5 Printers and Photocopiers

- To avoid accidentally printing to an unintended network device, computer users should additionally check that their default printer is correct before printing any documents;

- Sensitive personal data must be cleared from printers and photocopiers immediately on completion. If these are no longer required, the items must be shredded or sent for secure disposal;

- It is the responsibility of the person who sends information to be printed to ensure they collect their documents and not leave them unattended. If information is of a confidential/sensitive nature and it is misplaced or missing, this should be reported to the Information Governance Team.

4.6 Keeping Desk / Word Areas Clear

It is essential all staff in offices or sharing office space with external partners adopt strict clear desk and clear screen practices to reduce or remove the risk of unauthorised access, loss, theft and damage to information. This is both during and out of normal working hours.

Working at a desk or workstation will provide a comfortable working position and help avoid information security risks. Here are some ways for you to manage your workspace that will also make sure you remove risks to data security:

- Try not to let piles of useful information accumulate instead of being returned to drawers and filing cabinets;

- Be aware that people around you including visitors to your floor have opportunities to view information that should not be seen. When away from your desk, turn off or lock your monitor;

- Avoid clutter. Important paperwork can get mixed up and filed in the wrong place, lost or thrown away instead of being disposed of properly. Removable media like CDs, DVDs and USB sticks are easily damaged or lost. Do you really need all of those Post-it notes? Can you hold any of this information electronically?

- Hanging on to information for too long means that out-of date information is still to hand and could still be used. This isn't only for paper clutter. 'Decluttering' drives and shared drives is also important. If you've closed a file or finished a piece of work, does all the obsolete information and related correspondence need to be kept or can it be destroyed or archived?

To remind you of the SFRS Secure Desk Policy, please click here.

5. NETWORK PASSWORD

Passwords must be strong and confidential as they are an important aspect of computer security. A poorly chosen or compromised password may result in unauthorised access and exploitation of SFRS resources.

5.1 Password Handling

Passwords for all systems are subject to the following rules:

- No passwords are to be spoken, written, e-mailed, hinted at, shared or in any way known to anyone other than the user involved;
- No passwords are to be shared in order to 'cover' for someone out of the office;
- Contact the ICT Service Desk to create a temporary account if there are resources you need to access;
- Passwords are not to be displayed or concealed on your workspace.

5.2 Password Composition

- Users will be prompted to change their passwords every 90 days;
- Users cannot use their previous 5 passwords when resetting;
- Passwords must have a minimum 8 characters;
- Passwords must contain a minimum 1 x upper case, 1 x lower case and 1 x number;
- Your account will lock out after 3 tries. Your account will reset after 15 minutes. You can then try to remember your password or contact the SFRS ICT Service Desk to reset;

- Users who have a smartphone or tablet device must change the password to reflect their new network password to allow email synchronisation to complete;

- When creating a password, ensure it does not contain malicious or offensive wording.

5.3 Creating Strong Passwords

A strong password:

- Does not contain your user name, real name or company name;

- Does not contain the use of postcodes, house numbers, phone numbers, birthdates, ID card numbers, social security numbers, etc.;

- Does not contain a complete word;

- Is significantly different from previous passwords;

- Contains characters from the composition listed in section 5.2 of this guidance.

To remind you of the SFRS Network Password Policy, please click here.

6. SECURE EMAIL

The security of electronic information is critical in today's environment, with potential interception of unsecured email sent over the internet being a realistic possibility. To mitigate this risk, any electronic personal or sensitive information should be secured in transit. As such, all SFRS employees are responsible for taking the appropriate steps, as outlined below, to use the correct method of email appropriate to the content and recipient(s).

Data Protection is of concern regarding secure emails, as any sensitive information sent by email that is not sent on a secure system is open to interception as the email travels across the internet to the recipients' email systems. By sending this information by a secure email service, only the intended recipient will be able to access the information and, in the event the message was intercepted, the content could not be read due to the encryption protection applied.

6.1 Egress Switch Secure Email System

- Egress Switch is a UK Government CPA Foundation Grade certified email encryption product which means it is suitable for sharing OFFICIAL and OFFICIAL-SENSITIVE under the Government Classification Scheme. As a result, Switch helps fill the gap between existing accredited government networks and external delivery partners, citizens and third sector businesses;

- This is the current and only secure email system available within SFRS.

Should you have any queries regarding Secure Email, please contact Lynne McAlonan, the Information Security Officer at lynne.mcalonan@firescotland.gov.uk.

7. ASSOCIATED DOCUMENTS / REFERENCES

Acceptable Use Policy
Code of Conduct
Disciplinary Policy and Procedure
Network Password Policy
Secure Desk Policy

Data Protection Act 2018