mental welfare commission for scotland

Policy Title: Information Risk Management Policy	**Policy Number:** 057
Issue Number:	**Date of First Issue**: October 2009
Date of last review: August 2020	**Date of next review:** August 2021
Approved by: OMG	**Lead Person:** Information Governance Manager

1. Introduction

Incidents involving the loss of personal/sensitive/confidential material can cause damage to an organisation's image and reputation and can have implications, some serious, for individual members of staff. More importantly, such incidents can cause distress and embarrassment to individuals whose data has inadvertently been made public.

This policy highlights where major areas of potential information loss lie and what action can be taken to mitigate those risks. Commission staff have a duty to protect information entrusted to them. Adopting some basic ground rules will offer protection to individuals whose information we hold, and to individual staff and the Commission, from the unwanted consequences of information loss.

The National Confidential Forum, (the NCF) was established as a Committee of the Commission in 2014 under the Victims and Witnesses (Scotland) Act 2014. This Act amends the Mental Health (Care & Treatment)(Scotland) Act 2003 to allow for the NCF to be a committee of the Mental Welfare Commission for Scotland. The NCF's core function is to receive and listen to testimony from those who were in institutional care as children.

The Commission's Information Risk Management Policy also covers the NCF. The Commission is data controller for the NCF. In this policy, statements made about information risk at the Commission apply equally to the NCF. There are some minor variations between the NCF and the Commission with respect to the more operational aspects of data protection and these are not reflected in this policy. These differences are managed at an appropriate level within the respective organisations.

This Policy should be read in conjunction with other Commission policies such as the IT Security Policy (4), IT Code of Conduct (5), Mobile Device Policy, Data Breach Policy (66) Data Protection Policy (29), and the Flexible Mobile Working (42).

Staff are required to undertake mandatory cyber security and GDPR/data handling training available as modules from the LearnPro e-learning platform.

Any member of staff who is deemed to be in breach of the Information Risk Management Policy may be subject to disciplinary measures.

2. Office security

The Commission recognises that, in order to carry out its role effectively, staff need to access and use sensitive information. Staff have a duty to ensure that the information is kept secure and only used for the purpose intended.

Within Thistle House, this information is protected in a number of different ways, including:

- Internal door security, accessible only by swipe card
- Password protected computer equipment
- Clear desk policy
- Lockable storage facilities

Within NCF's Glasgow Office similar security measures are in place. In addition to these, the NCF office also has a large safe for storage on short-term basis for personal data retained in relation to hearings.

3. E-mail, Cloud Storage, FAX, answering machines, memory sticks (and other portable storage devices), social media, using personal equipment.

3.1 E-mail

The Commission uses NHS mail and this means that transactions of personal data between MWC and .nhs.net accounts and between some, but not all, government accounts (e.g. gsi.gov.uk and gsx.gov.uk) are encrypted and acknowledged to be secure. **Further guidance on when sensitive patient data and staff identifiable information can be sent by email is contained in paragraphs 15 and 16 of the IT Code of Conduct and guidance on the use of NHS mail is available from the intranet**.

Double check the recipient email address, and be careful when using the autocomplete function. Encryption does not prevent human error. Sending an email to the wrong person could be a data breach if it contains personal information.

Advice on email use can also be obtained from the Systems Administrator or IT Support Officer.

When in doubt about whether the addressee of an email is using an encrypted email address, staff should type [Secure] in the subject of their email. Full instructions on this facility are available from the intranet.

Staff of the NCF forum have not transferred across to the NHSmail system and so should seek advice directly from their service provider regarding the acceptable use of email or the use of encryption tools to secure sensitive data in transit.

The current service provider is Talon http://talonhit.com/.

It is unacceptable to use personal email or an email account provided by another organisation to transfer or process Commission data.

3.2 Cloud Storage

Commission information must never be transmitted or stored in internet storage locations e.g. DropBox, GoogleDrive, SkyDrive.

3.3 FAX

We discourage the use of FAX to transfer data, especially sensitive, personal data. If you have to FAX and have explored all other alternatives then you must first read the published guidance available from NHS Scotland staff on the use of faxes;
Guidance on the use of facsimile transmissions for the transfer of personal health information within the NHS in Scotland. MEL (1997) No. 45

3.4 Answering machines

Be wary of leaving messages of a personal, sensitive nature on a telephone answering machine. Better to ask the individual to call you back than to leave a message on a phone that could be accessed or overheard by other individuals or, if you have dialled the number incorrectly, risk this message been accessed by the wrong person/organisation.

3.5 Memory sticks (and other portable memory devices)

The Commission has purchased a small number of USB memory sticks which staff can borrow from the Commission IT team. These memory sticks are encrypted to a level that meets current internationally recognised standards.

Portable storage devices should not be used for downloading and/or transporting sensitive personal information. These are too easily lost or stolen. Commission staff are expressly expected not to do this unless a business case has been made, and approval obtained, for what is proposed. Advice on this can be obtained from IT staff (IT Code of Conduct, para. 17).

Some staff have been provided with mobile phones which enable them to receive and respond to calls and to access and respond to Commission emails when working away from the office.

3.6 Social Media

Staff must not issue or transmit any Commission data or information via social media sites or web services without the explicit consent of a member of the Commission Executive Team. (see the Media and Social Media Policy for more information)

3.7 Using personal computer devices

Commission staff should **not** use personal devices to access Commission data. Encrypted laptops are provided for this purpose if required. They must not use a non-Commission mobile phone, ipod / ipad or tablet device to store or transmit Commission data.

4. Patient files and high risk information.

As stated explicitly in the IT Security Policy and IT Code of Conduct, Patient files and any other high risk information as defined in the Agile work (Policy 42) guidance should never leave the office in physical format.

The only exceptions to this are for members of staff who need to take high risk information away from Commission premises as a necessary part of their job, such as files for a major investigation.

In that case, only take the minimum paperwork necessary to carry out your task. Do not take the full file just because it's more convenient to do so. If you cannot avoid taking home the full official record, ensure that your supervisor is aware and has agreed to this. **Ensure that you note the paperwork that has been taken out the office in the register.**

IMP is available from laptops, which are encrypted to ensure that they are secure. The use of any other portable devices to store or transport patient sensitive information or information which should not be made public is not permitted under any circumstances.

Staff who intend to access information from the Commission's databases when out of the office should re-familiarise themselves with the guidance in the IT Code of Conduct, the IT Security Policy, the Mobile Devices Policy and the Information Management Risk Policy before doing so.

5. Working from Home

You can only use authorised Commission laptops which must be encrypted. All information should be stored on the Commission computer network. You should work directly from/to the appropriate Commission servers using remote access facilities.

Your device will be setup to ensure that the computer operating system and applications are up to date with virus protection software and any relevant security patches.

This reduces the need to take paper information home.

If you must take personal information outside the normal Commission computing environment to your home, adhere to the following rules:

Your work area should be in a separate location to general 'living' areas. This location should not be able to be easily seen or accessed by people outside the home. For example, do not situate your work area or computer station next to a ground floor window.

- Make sure that information is not left where other occupants of your home can see it. Again, this would include placing your laptop near windows.
- Keep paper documents, files and portable encrypted media or devices containing information in a lockable cabinet wherever possible and make sure that this is locked when not in use. Wherever possible, physically protect laptops. You may do this by using a lock or cable to secure the laptop, or placing it in a locked cupboard or drawer when not in use.
- **Fully switch off laptops,** never just close the lid to laptops as this bypassed the update process and may make machines vulnerable to infection by new viruses.
- Staff should also turn laptops off, if they leave it unattended for any period of time. It is important to fully switch off laptops as this enables security settings to be updated.
- If you are taking sensitive information home, in any format, go there directly. This reduces the chances of losing the information on the way.
- Use an appropriate carrier. Documents or other portable encrypted media should be transported in a secure, lockable briefcase or bag. Laptops must be carried in a laptop bag or rucksack.

- Exercise discretion. Do not read sensitive documents on a bus, for example, or work on personal data on a train. Do not draw attention to the fact that you are carrying Commission information.
- Hard copies must be destroyed using the confidential waste facilities provided by the Commission.

Always bear in mind that, in order to comply with data protection principles and GDPR, personal information, in any format, should not be kept for any longer than is necessary for the purpose for which it was collected.

6. Staying overnight

Staff may be required to stay in overnight accommodation during the course of their work. It is the Commission's view that sensitive information should not be left overnight in a vehicle but should be transferred to the hotel room in which the member of staff is staying. This is felt to be the better of the two options though, it is acknowledged, not without an element of risk.

7. Non-patient sensitive information

Other types of sensitive information held and used by the Commission include details of staff names and addresses, pension and salary information, staff review/appraisal documentation and financial/budget information.

This information should be treated with similar consideration as patient sensitive information. This means that it should only be accessible to those who have need of it; it should be kept secure if in use outwith the office; and, if in paper format, it should be disposed of securely when there is no longer a use for it.

8. Using public transport

Staff using public transport, including air travel, need to be extra vigilant when they are carrying information in any format, particularly if that information is sensitive, confidential etc.

Staff may regard travelling by public transport as an opportunity to complete work. This could be opening up a laptop or accessing handwritten notes. Staff should be aware of the dangers associated with this if there are people in close proximity who are able to view the notes or read material on the screen. A common sense approach should be adopted at all times. Do not work on sensitive or confidential material. Anonymise the information you are writing/typing to ensure that personal details, or other sensitive information, are not revealed.

If you are travelling alone and need to leave your seat, your laptop should be shut down/notes closed and taken with you.

9. Using mobile phones

Staff need to be aware that, when using phones in public areas, discussion of sensitive matters should be avoided where there is any possibility of being overheard by a third party, since that party may be motivated to use the information they overhear or pass it on to others, e.g. the media.

Some staff at the Commission have been provided with smart phones. These are provided on the understanding that the individuals concerned have read and understood their obligations as described in the Commission's Mobile Device Policy.

10. Lockable bags/storage

The Commission will provide all relevant staff with a secure, lockable bag which **must** be used to transport paper documents and other media, e.g. back-up tapes, containing sensitive or confidential information outwith the office. Staff must also ensure that any sensitive or confidential information they have at home is stored appropriately.

11. Information loss & obligation to report data breaches to the Information Commissioner's Office (ICO)

Under GDPR, reporting of data breaches is mandatory and must be done within 72 hours of the organisation becoming aware of the incident. If personal information is lost, inadvertently leaked or made public, then the member(s) of staff involved **must** follow the guidance given in the Data Breach Policy.

Personal data breach - GDPR – ICO – Our obligations

- The GDPR introduces a duty on all organisations to report certain types of personal data breach to the ICO. You must do this within 72 hours of becoming aware of the breach, where feasible.

- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.

- You should ensure you have robust breach detection, investigation and internal reporting procedures in place. (see the Commission's Data Breach Policy) This will facilitate decision-making about whether or not you need to notify the relevant supervisory authority and the affected individuals.

- You must also keep a record of any personal data breaches, regardless of whether you are required to notify (The Commission has a central data breach log details of which are available from the intranet)

Useful links to ICO guidance on identifying and promoting breaches

What is a personal data breach and how should I respond if I think a breach has occurred?

Reporting a personal data breach

Published guidance

The Scottish Government and Cyber Resilience

https://www.gov.scot/publications/scottish-public-sector-supplier-cyber-security-guidance-sppn-2-2020/

Information Governance and Security Improvement Measures - 2015-2017

NHS Scotland Information Security Policy Framework - July 2015

Directorate for Health Finance and Information: eHealth Division – NHS Scotland Mobile Data Protection Standard - CEL 25 (2012) *Updated from Version 1, 2008*

Related Internal Commission Policies

Current versions of all policies are available from the Commission Intranet;

- No.4 I.T. Security Policy.
- No.5 I.T. Code of Conduct.
- No.18 Media and Social Media Policy
- No. 29 Data Protection Policy
- No. 66 Data Breach Policy
- No 42 Agile Working Policy
- No. 61 Mobile Device Policy