Gwybodaeth
Dan
Reolaeth

Gwynedd Council

INFORMATION SECURITY OPERATING PROCEDURE

3.0

June 2018

Information Management Service

Information Security Operating Procedure

1. Introduction

The Council handles thousands of different types of information each day. This varies from public documents to extremely sensitive and confidential information. This information is an important asset, which, like other important business assets, needs to be suitably protected.

In terms of personal and sensitive information, it is vital that we maintain the highest standards of security in order to give the citizens of Gwynedd confidence in our ability to handle their personal details and to ensure that the Council complies with relevant statutory requirements, in particular Data Protection legislation.

2. Objectives

The objective of this information security operating procedure is to ensure that all users and managers understand their own responsibilities for protecting any confidential and personal data they handle.

3. Scope

This policy applies to all directly and indirectly contracted staff and other persons working for the Council.

4. Definition

Personal information means any information, which relates to an individual. Sensitive information includes information about an individual's health, criminal record, ethnicity, religion, politics, genetics or biometrics, trade union membership, sex life or sexual orientation.

Confidential information can include non-personal information about contracts/commercial issues, legal transactions or discussions about policies.

5. Paper records containing personal and/or confidential information

Clear desk policy – Personal and confidential information

Personally identifiable or confidential information should not be left unattended on desks and should be removed from view when unsupervised. Documentation should be stored in a locked cupboard overnight with the key kept in a safe place.

Confidential or personal information should not be left on desks, printers, photocopiers or fax machines at the end of the working day.

Printing

Particular care should be taken when printing to a shared photocopier/printer to avoid picking up papers belonging to other members of staff.

Where available, the secure print facility should always be used to avoid these situations.

Faxing

Faxing should only be used when there is no alternative means of sending the information.

- A cover sheet marked 'Private and Confidential' should always be used which contains:
    - who the fax is for (a named person)
    - who the fax is from (your name, team and location) your phone and fax number.
    - an explanation of what to do if the fax has been received by the wrong person (e.g. contact you immediately, and do not read or share the contents with anyone else)

- Before sending the fax, the intended recipient should be telephoned to let them know a confidential fax is being sent

- The recipient should be asked to ring back to confirm receipt, or rung back after the fax has been sent

- If using a pre-programmed fax number, the right one should be chosen, and the pre-programmed numbers regularly checked to ensure that they are still correct

- If entering the number manually, it should be double checked to ensure it is the right number

Posting

- Ensure that the destination you are sending documents to is still in the same place – especially if the recipient is outside the Council.

- The address should be checked and documents sent to a named person if at all possible, and not to a department or team.

- A covering letter or a compliment slip should be enclosed with the information – DO NOT put records or data into an envelope by themselves

- There should be a return address on the back of the envelope – this will allow a wrongly delivered envelope to be returned without having to be opened

- The envelope should be sealed securely and marked **Private and Confidential**

- If practical, personal or other sensitive information should be sent by recorded delivery, and the tracking information kept.

- If possible, typed labels or envelopes with windows should be used (ensuring that only the address is visible) – problems may arise if handwriting is misinterpreted.

Handling paper records containing personal or confidential data out of the office

If staff need to use paper records containing personal or other confidential data out of the office, the records must be safe at all times. An encrypted laptop or other form of remote, secure access to information may be a safer alternative.

Basic principles when handling paper records containing personal or confidential data

- Any record taken out of the office should be logged – the log must identify where the record has been taken, when, why and by whom

- Records should be removed only where necessary, and only for the minimum time required

Practical steps

- The person carrying paper documents is responsible for their safety – even if they are carrying documents for someone else.

- Files or documents should be carried in an appropriate bag at all times when on the move i.e. sealable, waterproof bag should be used – an open shopping or carrier bag is never an appropriate way to carry personal data, or confidential or sensitive documents. Even if documents are held in a robust file, that file should be carried in a bag.

- Where records are routinely removed from the office, staff should be supplied with a lockable case or bag

- Where larger quantities of records are routinely removed from the office, they should be carried in a lockable wheeled case or bag

- The files or folders should be in good condition, and individual papers securely fastened inside them – if papers are falling out or the file is damaged, the file should be replaced or repaired before it is taken out

- Files or documents should never be inspected in the street or even in the car park – they should be carried inside the building and to a safe environment before being examined

- Personal records should not be read on public transport or anywhere else where you can be overlooked

- Documents should never be unattended and on show in a car or other vehicle

- Before leaving a building, car or public transport, and before driving away from any location where paper records have been used, staff should make a conscious check that their bags are with them.

- Paper records should never be left in a car overnight. If staff need to return home with documents containing personal or sensitive data, they should be taken into their home and kept safe.

Disposal of confidential waste

Any work containing personal or confidential information should be disposed of appropriately in accordance with the Disposal of Confidential Waste Policy

6. Information held on computer and stored in buildings

Passwords

Passwords must be protected at all times.

Passwords designated for individual use should not be displayed or made available to others by any other means.

User access privileges can be amended for those who require access to particular resources. In such cases, authorised requests should be presented to the IT Helpdesk.

Passwords will be required to be complex. There will be a minimum requirement of 12 characters containing upper and lower case lettering a number and a special character.

Any compromised passwords must be changed as soon as practically possible.

Passwords or log on information must not be written down or shared with anyone else.

Devices

Computers need to be locked (CTRL + ALT + DEL) when desks are left unattended.

Keyboard and screens should be angled away from areas to which the public have access and angled away from windows.

Third Party Access

Partner agencies or third party suppliers must not be given details of how to access the Council's network without following the appropriate authorisation path. Procedures for third party accounts, such as system support companies, are detailed in the third party access policy. User accounts relating to individuals from partner agencies who require connecting to the corporate domain must be authorised by Corporate Services Team.

Sending personal and confidential e-mails

- When sending an e-mail to an external address, consider whether the e-mail should be encrypted or password protected. The IT Service can provide assistance in this respect.
- When starting to type in the name of the recipient, Outlook might suggest similar addresses that have been used before. Make sure that the right address has been chosen before sending the email.
- When sending an e-mail to many different individuals at the same time, consider if it would be appropriate to use a blind carbon copy (bcc) rather than carbon copy (cc) so that their address is not revealed to the other recipients.
- Care should be taken when using a group email address. Check who is in the group and make sure you really want to send your message to everyone.
- Due consideration needs to be taken prior to printing email messages which contain confidential data as this introduces new risk vectors.

There is an Email Use Policy containing further detail.

Internet Access

- Internet access is granted to enable colleagues to access information or resources as part of their duties.
- When online, colleagues must take responsible steps to protect themselves and the Council's infrastructure from harmful content as well as loss of data or other damage resulting from their activities. This includes, but is not limited to, not visiting malicious or obscene sites, not posting malicious or obscene messages online and not downloading items of software from the Internet.
- No unauthorised third party storage resource should be used for the Authority's data unless the data is designed to be in the public domain.
- There are web filtering and anti-malware controls in place and no attempts should be made to circumvent or bypass these controls. The web filtering process includes HTTPS inspection so that encrypted traffic can reviewed for malicious content, this does not include items such as online banking and communication for user confidentiality.
- Personal use of the Internet is allowed but this should be restricted to officially agreed break periods and should not affect any individual's duties.
- Logs of Internet usage are maintained and can be used in the event of disciplinary cases.
- There is an Internet usage policy containing further detail.

Physical access

Buildings must have appropriate control mechanisms in place for the type of information and equipment stored there. This means:

- Identification and access tools/ passes (e.g. badges, keys, entry codes etc.) must only be held by officers authorised to access those areas and should not be loaned/ provided to anyone else.
- Visitors should be required to sign in and out with arrival and departure times and required to wear an identification badge.

Building Clearance

- In any building closure, office move or relocation, it is essential that all papers records containing confidential and sensitive information are either removed and disposed of appropriately or relocated. **If you are the information asset owner (i.e. the manager of the service that is moving) it is your**

responsibility to ensure the security of that information throughout the relocation process.

- Contact the Information Management Service for advice.
- No documents should be left behind at the property.
- Similarly, any computer equipment should also be removed.

7. Verbal Information Sharing

Information obtained at work should be used for work purposes only. Personal details about individuals should not be discussed with other staff who are not involved with the case/matter. Confidential issues should not be discussed out in the open in public places nor with family and friends.

When sharing information over the phone, it should be ensured that the recipient is authorised to receive the information.

8. Software and Storage of Information

All items of software installed on corporate devices must be supported and subject to patches and updates. Any items not corresponding to the Council's security standard must be upgraded, replaced or deleted.

Requests and queries relating to new items of software must be presented to the IT Service for review and guidance.

All items of software must be installed and configured by the IT Service.

The Council provides a secure environment for business files and sensitive data and this should not be compromised by using third party solutions e.g. Dropbox, whose security cannot be guaranteed.

All business data must be stored on storage that has been approved by the Council.

Password protecting files is discouraged as passwords are often lost and procedures of informing others of the passwords often undermine security measures. Protecting data in files and systems must be facilitated using logical access rights.

9. Removable Media and Laptops

Removable media include, but are not restricted to the following:

- CDs
- DVDs
- Optical Disks
- External Hard Drives
- USB Memory Sticks
- Media Card Readers
- Embedded Microchips
- MP3 Players
- Digital Cameras
- Backup Cassettes
- Audio Tapes

Due to the risks of introducing a virus, the above may only be purchased via IT and only if a valid reason for their use is received. For USBs, contact the Help Desk for a form which should then be e-mailed to USB@gwynedd.llyw.cymru.

Special care must be taken to physically protect the removable media device and stored data. Anyone using removable media devices must be able to demonstrate that they took reasonable care to avoid damage or loss.

If information is stored in one place, i.e. only on the removable device, there is a higher risk of loss since there is no back-up copy. Information should always therefore be backed up elsewhere e.g. on the network.

Removable media devices that are no longer required, or have become damaged, must be disposed of securely. (see Appendix B in the confidential waste disposal policy referred to above).

Only corporately owned or approved devices should be connected to corporate computers.

10. Remote and Home Working

Remote workers must ensure that Council owned, portable computer devices are connected to the corporate network at least once a month to enable the anti-virus software and group policies to be updated.

Portable computer devices include, but are not limited to, the following:

- Laptop Computers
- Tablets
- Mobile Phones

Remote Working guidelines contain further detail.

11. Information Security Breaches

If any personal or sensitive information is lost/stolen, compromised or disclosed in error this must be reported to your line manager or the Information Manager immediately.

Breaches that cause a high risk to data subjects must be reported to the Information Commissioner within 72 hours of the you being made aware of the breach.

Serious breaches, which includes unauthorised disclosures/loss or theft of personal information may result in the Council being fined up to €20 million by the Information Commissioner's Office.

12. Responsibilities for Information Security

Every member of staff is responsible for information security. Failure to make appropriate arrangements to secure personal or sensitive information may be considered as gross misconduct and therefore would be dealt with in accordance with the Council's disciplinary policy and procedure.

If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

The Information and Security Management Group is responsible for overseeing the information security operating procedure and for ensuring it is adhered to by all departments through the relevant Heads of Department.

Heads of Department are required to implement this operating procedure in respect of both paper and electronic systems operated by their departments and are responsible for ensuring that staff, and other persons authorized to use those systems are aware of and comply with it and associated policies, i.e.

- Information Management Policy
- Data Protection Policy
- Disposal of Confidential Waste Policy

The Senior Information Risk Owner (SIRO), Head of Corporate Support, has ultimate responsibility and accountability for the security of the Council's information assets.

13. Responsibilities of Managers

In addition to the above, managers have the following responsibilities:

- Ensuring that all staff members receive appropriate information security awareness training and regular updates as relevant for their role.

- Reviewing user access rights at regular intervals to ensure that the appropriate rights are still allocated.

- Ensuring that appropriate arrangements are made to secure information when a member of staff leaves or changes jobs.

14. Legal Responsibilities

The following statutory legislation governs aspects of the Council's information security arrangements. This list is not exhaustive:

Legislation	**Areas Covered**
The Electronic Communications Act 2000	Cryptography, electronic signatures
The General Data Protection Regulation and Data Protection Act 2018	Protection and use of personal information
The Copyright Designs and Patents Act 1988	Software piracy, music downloads, theft of Council data
The Computer Misuse Act 1990	Hacking and unauthorised access

15. Review

The procedure will be reviewed in 2 years' time.