Information Management and Protection Policy

Information Governance Policy

November 2020

Version Number	5.0
Approved by	Corporate Policy and Resources Committee
Date approved	15/10/2020
Authorised by	Director of Resources
Contact Officer	Information Governance Officer

Revision History

Revision Date	Revised By	Previous Version	Description of Revision
29/9/2011	S M Anderson	Draft V0.3	Adopted by Policy and Resources Committee
1/9/2012	S M Anderson	Version 1.0	Reviewed – Sponsor Approval removed pending restructure.
6/2/2014	S M Anderson	Version 2.0	Reviewed and amended to incorporate changes to IG organisation (Paras 10.2 and 10.4). Amended to include references to Public Service Network (PSN). Minor changes and corrections.
23/6/2014	S M Anderson	Version 3.0	Reviewed by Corporate Information Governance Group. Minor changes and corrections. Approved by CMT.
9/2/2017	Corporate Information Governance Group	Version 4.0	Amendments resulting from review: New Government Classifications included; organisation changes included; job titles updated; 5 new risks added; review period extended to 2 years; paras renumbered and minor typographical corrections.
15/10/20	J I Bingham	Version 5.0	Change to terminology throughout document Section 11: Change job roles and responsibilities Section 2.4: Change of Breach Description in line with the UK GDPR

Contents

1. Foreword by the Chief Executive

Information is the life blood of West Lindsey District Council. Without it, our jobs would be impossible to do.

To operate efficiently, we must collect and use information about people with whom we work. This may include members of the public, current, past and prospective employees, elected members, clients and customers, and suppliers. In addition we may be required by law to collect and use information in order to comply with the requirements of central government.

All personal information must be handled and dealt with properly, no matter how it is collected, recorded and used, and whether it is on paper, in computer records or recorded by any other means. We all have a responsibility for its safe handling.

This document sets out the principles of information management and data protection, our responsibilities, the access rights of individuals, information sharing and complaints. I endorse it wholeheartedly.

Ian Knowles
Chief Executive
West Lindsey District Council

2. Policy Statement

2.1 West Lindsey District Council (the Council) will create an environment where:

- information, in any form, is valued as a corporate asset;
- organisational boundaries are invisible and information is freely shared in a way that preserves the context, integrity, sensitivity and security of the information asset while making sure that all staff have access to accurate and appropriate information that they need for their job; and
- Information that has reached the end of its useful life is either kept permanently in a secure archive or is destroyed in accordance with the Council's Retention and Disposal Schedule.

3. Key Messages

- The Council must draw up and maintain inventories of all important information assets.
- All information assets, where appropriate, must be assessed and classified by the owner in accordance with the Council's Protective Marking Scheme.
- All personal information must be collected, processed and protected in accordance with the General Data Protection Regulations.

- Access to information assets, systems and services must be conditional on acceptance of the appropriate Acceptable Usage Policy.
- Users should not be allowed to access information until the Team Manager, People and Organisational Development is satisfied that they have read all relevant Information Governance Policy documents, have completed relevant awareness training, and understand and agree the legislated responsibilities for the information that they will be handling.
- Personal, confidential or sensitive information must be classified OFFICIAL-SENSITIVE in accordance with the Council's Protective Marking Scheme and must not be disclosed to any other person or organisation unless an appropriate Information Sharing Agreement is in place.
- OFFICIAL-SENSITIVE information must not be shared via any insecure methods including unencrypted email, USB sticks, CD/DVDs or by paper based methods, fax and telephone.
- The disclosure of personal, confidential or sensitive classified information in any way other than via Secure email or other approved secure transmission method may result in disciplinary action.
- Data breaches and information security incidents must be reported and managed immediately in accordance with the Information Security Incident Management Policy to minimise the effect on the affected subject and the Council and its partners.

4. Purpose

4.1 Information is a principal asset of the Council. This Policy is the foundation on which all information-related activity is built. It aims to allow information to be managed and protected from creation or acquisition to destruction or permanent archive, taking into account its security, storage, access, distribution, use, presentation and retention.

4.2 Implementation of the Information Management and Protection Policy will make sure the Council complies with all relevant legal requirements and provide a framework for the use and protection of information in line with good practice.

5. Scope

5.1 This Policy applies to all full time and part time employees of West Lindsey District Council, elected members, partners, contracted employees, third party contracts (including agency employees), volunteers, and students or trainees on placement with the Council.

5.2 The Policy applies to all information created or held by the Council, in whatever format (e.g. paper, electronic, email, microfiche, film) and however it is stored (for example ICT system/database, shared drive

filing structure, email, mobile devices, removable media, filing cabinet, shelving and personal filing drawers).

6. Risks

6.1 The Council recognises that there are risks associated with users accessing and handling information when carrying out official Council business.

6.2 This Policy aims to mitigate the following risks:

- Sensitive and confidential data security breaches caused by failure to properly classify and handle information could result in distress to individuals, regulatory fines and damage to the Council's reputation.
- Personal, sensitive, or bulk information is released into the public domain through a failure to properly protect OFFICIAL-SENSITIVE information could result in distress to individuals, regulatory fines and damage to the Council's reputation.
- Information disclosed, stolen, misused or lost when being passed between Council departments or to partners through a lack of information sharing control could result in distress to individuals, regulatory fines and damage to the Council's reputation.
- Failure to report data protection breaches and information security incidents could result in missed opportunities to correct inadequate processes leading to repeat incidents and possible regulatory fines and damage to the Council's reputation.;
- Inadequate destruction of data through lack of training and awareness could result in distress to individuals, regulatory fines and damage to the Council's reputation.

6.3 Non-compliance with this Policy could have a significant effect on the reputation and efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

7. Principles of the Information Management and Protection Policy

7.1 The information collection, storage, analysis and exchange processes within the Council should embody the following principles:

- **We treat information as a West Lindsey District Council resource**. Information, regardless of where it is held, is a corporate resource and hence the property of the Council and not the property of individuals. All information resources and processes must add value to the work of the Council and demonstrate value for money;

- **We are all responsible for the Council's information assets**. Those with specific responsibility for managing information assets must be clearly identified. However, all users are accountable for their use of information;

- **We will share information (responsibly) with our colleagues, partners and customers**. Staff should be able to access information for the effective performance of their job and there should be the opportunity for the free flow of information, as appropriate, across the Council;

- **We keep records of what we do and retain them in the most cost effective way**;

- **The information we produce must be accurate and meet our customers' expectations**. Information must be timely, relevant and consistent, with duplication of information kept to a minimum; and

- **Our information complies with our statutory obligations**. Information management and protection must comply with current legislation, information must be managed in accordance with Council policies, standards and procedures and information must be kept secure as appropriate.

8. Information Management and Protection Framework

8.1 This Policy should be read in conjunction with the following related policies. The interrelationship of these policies and other corporate policies and frameworks is shown at Appendix 1:

- Legal Responsibilities Policy;
- Information Security Policy;
- Information Security Incident Management Policy;
- Data Protection Policy;
- Data Breach Policy;
- Freedom of Information and Environmental Information Policy;
- Information Sharing Policy; and
- Data Quality Policy.

9. Applying the Policy

9.1 The Council will develop effective procedures and processes to comply with this Policy. In particular, the Council will manage and protect information assets by:

- detailing how information assets should be identified;
- specifying how information assets should be classified and protectively marked;

- assigning information asset owners;
- defining the acceptable use of information assets;
- specifying how information should be stored;
- specifying how information should be disclosed or shared;
- requiring personal information to be identified and protected; and
- detailing the steps to be taken in the event of personal information being lost or compromised.

9.2 For further information on how to apply this Policy, refer to Appendix 2.

10. Desired Outcomes

10.1 The Council will have a comprehensive system of integrated policies, standards and procedures in respect of information, supported by information capture, storage, analysis and exchange systems that will allow all Council staff to:

- conduct their daily business efficiently and effectively;
- have timely access to meaningful and appropriate information;
- operate within the requirements of current legislation;
- support and inform Council decision-making; and
- Respond appropriately to information and data requests.

11. Policy Governance

11.1 It is for Members to approve the Information Management and Protection Policy and for the Senior Management Team to approve and implement the procedures underpinning the Policy.

11.2 The Monitoring Officer is the nominated board-level person responsible for information governance.

11.3 The Senior Information Risk Owner (SIRO) is a member of the Management team and is responsible for managing the Council's information risks.

11.4 The Data Protection Officer is responsible for setting and implementing the Council's Data Protection Policy and determining complaints relating to requests for information and is responsible for co-ordinating implementation of the Policy. The Legal Responsibilities Policy summarises the legislation relevant to the Council's information assets.

11.5 The Corporate Policy Manager is responsible for managing the day-to-day activities around data protection and freedom of information.

11.6 Team Managers are responsible for determining and signing-off requests under the Freedom of Information Act 2000 and the Environmental Information Regulations that relate to their service area. The Council's

policies for providing information under these regulations are detailed in the Freedom of Information and Environmental Information Policy.

11.7 Team Managers are also responsible for making sure their staff are aware of their responsibilities with regard to the management and protection of information and comply with all relevant policies listed at paragraph 5.

11.8 All employees are responsible for following the procedures underpinning this Policy relating to requests for information and the daily management of the information and records which they generate in the course of their work.

12. Policy Compliance

12.1 If any user is found to have breached this Policy, they may be subject to the Council's disciplinary 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).

12.2 If you do not understand the implications of this Policy or how it may apply to you, seek advice from the People and Organisational Development Team.

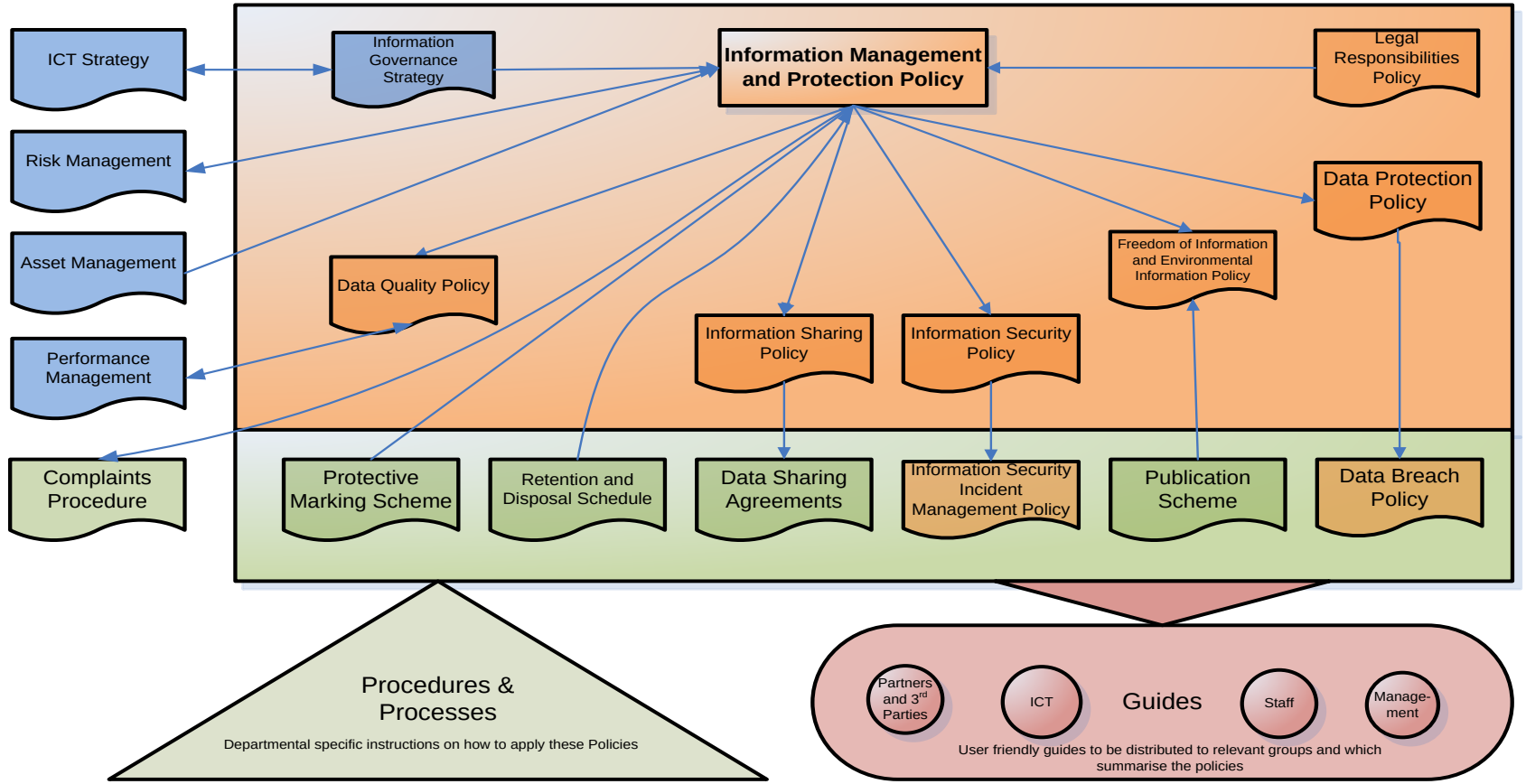
13. Training and Education

13.1 Standards, procedures and guidance will be developed as appropriate to support this Policy. The Council will provide staff with the necessary information based skills and training required for them to undertake their roles effectively, efficiently and in accordance with this and other supporting policies, standards and procedures.

14. Review

14.1 This Policy will be reviewed every two years from the date of its adoption.

Appendix 1 – Information Management and Protection Framework



Appendix 2 – Guidance for Applying this Policy

2.1 Information Asset Management

2.1.1 Identifying Information Assets

The process of identifying important information assets should be sensible and pragmatic.

Important information assets will include, but are not limited to, the following:

- Filing cabinets and stores containing paper records
- Computer databases
- Data files and folders
- Software licenses
- Physical assets (computer equipment and accessories, personal digital Assistants, mobile and smartphones)
- Key services
- Key people
- Intangible assets such as reputation and brand

The Council must draw up and maintain inventories of all important information assets that it relies upon. These should identify each asset and all associated data required for risk assessment, information/records management and disaster recovery. At minimum it must include the following:

- Type
- Location
- Designated owner
- Security classification
- Format
- Backup
- Licensing information

2.1.2 Classifying Information Assets

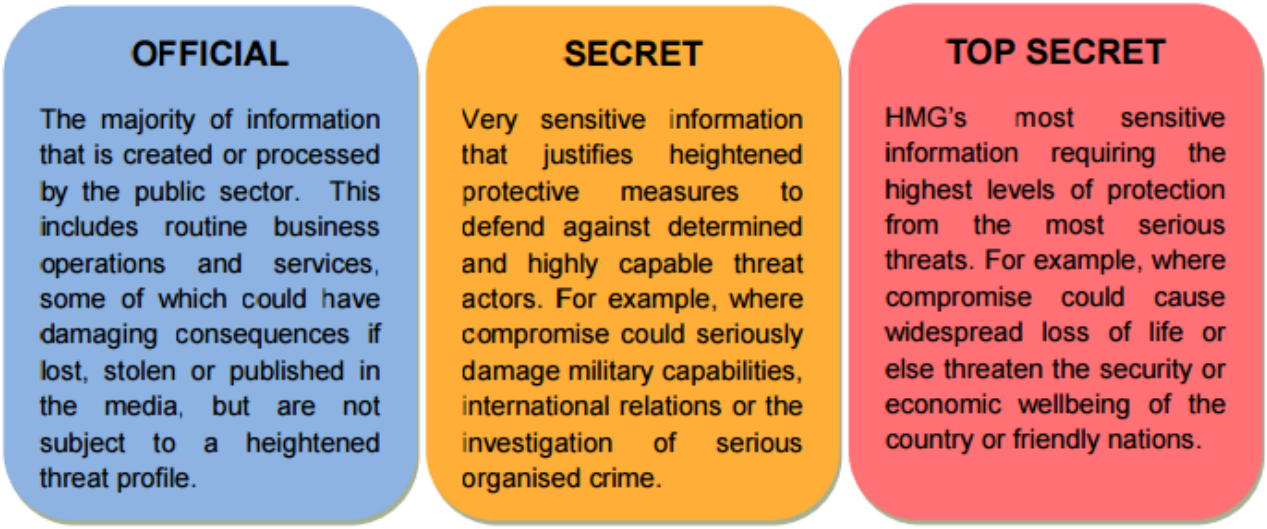
On creation, all information assets must be assessed and classified by the owner according to their content. At minimum all information assets must be classified and labelled in accordance with the Council's Protective Marking Scheme (PMS). The classification will determine how the document should be protected and who should be allowed access to it. Any system subsequently allowing access to this information should clearly indicate the classification.

The Council's PMS formally adopts the Government Security Classifications issued on 1 Oct 2014. This describes how to classify information and apply

protective markings. The way the protectively marked document is handled, published, moved and stored will depend on this scheme.

The three classifications are:

- OFFICIAL
- SECRET
- TOP SECRET



A limited subset of OFFICIAL information could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media. This subset of information should still be managed within the "OFFICIAL" classification tier, but may attract additional measures (generally procedural or personnel) to reinforce the "need to know". In such cases where there is a clear and justifiable requirement to reinforce the "need to know", assets should be conspicuously marked: "OFFICIAL–SENSITIVE".

A district council is only normally authorised to handle OFFICIAL and OFFICIAL-SENSITIVE material.

Within the **Official-Sensitive** classification, there are three additional descriptors which can be used:

1) **Personal**: The information relates to an individual or group, and inappropriate access to this documentation could have damaging consequences.

2) **Commercial**: The information is commercially sensitive and includes statutory or regulatory requirements.

3) **LocSen** (Locally Sensitive): The information is sensitive to a specific region and shouldn't be accessed by users in other geographic regions (unlikely to be relevant to a district council).

While these descriptors are not mandatory, it is best practice to apply them where necessary.

2.1.3 Key Classification Principles

There are four key principles that govern classification:

1) **All government information has intrinsic value and should be classified**.

   The onus should be on the document creator/owner to prove that the information is useful, required, and in regular use. If it isn't, it should be removed from the repository.

2) **Everyone who has access to government information has a duty of confidentiality and should protect it regardless of classification**.

   Although the GSC categorises public sector documents as Official by default, your information will be more secure if you treat it as being at the highest level of security that your repository allows, unless specifically marked. For example, if the repository is selected as being suitable for Secret documents, then all documents should default to Secret unless specifically classified otherwise. It is also recommend checking the classifications on a regular basis to ensure that appropriate security it provided.

3) **Access should only be granted on the basis of a genuine "need to know."**

   When managing permissions, think about why each user needs access to the information. Permissions should only be granted when absolutely necessary, then revoked once the need is gone.

4) **All information exchanged between internal and external partners should undergo the same protection and conform to the relevant legislative and regulatory requirements.**

   If you share information, you must take responsibility to ensure you are aware of and follow required rules, policies, and processes. Also, organisations should take steps to make it possible for parties to safely share information externally without breaking those rules. The organisation's infrastructure should be flexible enough to allow you to do this without compromising the security of the environment.

2.1.4 Personal Information

Personal information is any information about any living, identifiable individual. The Council is legally responsible for it. Its storage, protection and use are governed by the General Data Protection Regulations. For the purposes of

the Regulations, the Chief Executive is the “Data Controller” and further details and specific requirements can be found in the Data Protection Policy.

2.1.5 Assigning Asset Owners

All important information assets must have a nominated owner and should be accounted for. An owner must be a member of staff whose seniority is appropriate for the value of the asset they own. The owner’s responsibility for the asset and the requirement for them to maintain it should be formalised and agreed.

2.1.6 Information of Limited or No Practical Value

Items of information that are of limited or no practical value should not be assigned a formal owner or inventoried. Information should be destroyed if there is no legal or operational need to keep it and temporary owners should be assigned within each department to ensure that this is done. Guidance on the retention and disposal of information can be found in the Retention and Disposal Schedule.

2.1.7 Information Assets with Short Term or Localised Use

For new documents that have a specific, short term localised use, the creator of the document will be the Document Owner. This includes letters, spreadsheets and reports created by staff. All staff must be informed of their responsibility for the documents they create.

2.1.8 Corporate Information Assets

For information assets whose use throughout the Council is widespread and whose origination is as a result of a group or strategic decision, a corporate owner must be designated and the responsibility clearly documented. This should be the person who has the most control over the information.

2.1.9 Acceptable Use of Information Assets

The Council must document, implement and circulate Acceptable Use Policies (AUP) for information assets, systems and services. These should apply to all full time and part time employees of West Lindsey District Council, elected members, partners, contracted employees, third party contracts (including agency employees), volunteers, and students or trainees on placement with the Council. Use of the system must be conditional on acceptance of the appropriate AUP. This requirement must be formally agreed and auditable.

As a minimum this will include:

- Email Policy.
- Internet Acceptable Usage Policy.
- Computer, Desk and Telephone Policy.

- Remote Working Policy.
- Removable Media Policy.

2.2 Information Storage

All electronic information will be stored on centralised facilities to allow regular backups to take place.

Records management and retention guidance will be followed.

Staff should not be allowed to access information until their line manager is satisfied that they understand and agree the legislated responsibilities for the information that they will be handling. The legislated responsibilities of elected members' are detailed in the Member Code of Conduct.

Databases holding personal information will have a defined security and system management procedure for the records and documentation.

This documentation will include a clear statement as to the use, or planned use of the personal information.

Files which are identified as a potential security risk should only be stored on secure network areas (contact the ICT help-desk for advice).

2.3 Disclosure of Information

2.3.1 Freedom of Information and Environmental Information Regulations

The Council takes its responsibility to promote open and transparent government seriously. Wherever possible, and subject to relevant legislation, the Council will provide ready access to the information it holds.

The Council's Policy on providing information is detailed in the Freedom of Information and Environmental Information Policy.

2.3.2 Sharing OFFICIAL-SENSITIVE Information with other Organisations

OFFICIAL–SENSITIVE information must not be disclosed to any other person or organisation via any insecure method including, but not limited to, the following:

- Paper based methods.
- Fax.
- Telephone.

Where information is disclosed/shared it should only be done so in accordance with a documented Information Sharing Protocol and/or Data Sharing Agreement.

Disclosing OFFICIAL-SENSITIVE information to any external organisation is also prohibited, unless via a secure email. Emails sent between west-lindsey.gov.uk addresses are held within the same network and are deemed to be secure. However, emails sent outside this closed network travel over the public communications network (Internet) and are liable to interception or loss. There is a risk that copies of the email are left within the public communications system.

Secure email accounts must be used for communicating OFFICIAL-SENSITIVE material. For further information see the Email Policy.

An official email legal disclaimer must be contained with any email sent. This can be found in the Email Policy.

The disclosure of OFFICIAL-SENSITIVE information in any way other than via Secure email is a disciplinary offence. If there is suspicion of a councillor or employee treating OFFICIAL-SENSITIVE information in a way that could be harmful to the Council or to the data subject, then it is be reported in accordance with the Information Security Incident Management Policy, and the person may be subject to disciplinary procedure.

Any sharing or transfer of Council information with other organisations must comply with all legal, regulatory and council policy requirements. In particular this must be compliant with the Data Protection Act 1998, The UK GDPR, The Human Rights Act 1998 and the Common Law of Confidentiality.

2.4 Breaches of the UK GDPR

A breach of the UK General Data Protection Act (GDPA) is defined as:

“A breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised discloser of, or access to personal data transmitted, stored or otherwise processed.”

The Council will always treat any data breach as a serious issue, potentially warranting a disciplinary investigation. Each incident will be investigated and judged on its individual circumstances, addressed accordingly and carried out in line with the employee code of conduct.

All breaches of the UK GDPR must be investigated. Serious breaches must be reported to the Information Commissioner’s Office (ICO) in line with ICO guidance.

The procedure to be followed on discovering a breach of the UK GDPR is detailed in the Data Protection Breach Policy. To minimise the effect of the

breach on both the affected party and the Council it is essential that the actions detailed in the Policy are carried out immediately.

2.5 Information Security Incident Management

An information security incident includes, but is not restricted to, the following:

- the loss or theft of data or information;
- the transfer of data or information to those who are not entitled to receive that information;
- attempts (either failed or successful) to gain unauthorised access to data or information storage or a computer system;
- changes to information or data or system hardware, firmware, or software characteristics without the Council's knowledge, instruction, or consent;
- unwanted disruption or denial of service to a system; and
- the unauthorised use of a system for the processing or storage of data by any person.

All information security incidents must be reported and investigated in accordance with the Information Security Incident Management Policy which is a supporting policy of the Information Security Policy.