INFORMATION SECURITY POLICY

Title	Information Security Policy
Owner	Data Protection Officer/IT Manager
Issue date	August 2019
Next revision due	August 2020

Contents

1. Introduction

1.1 All information held by the council, in all formats, represents an extremely valuable asset and, therefore, must be used and stored in a secure manner.

1.2 The Policy must be read in conjunction with other Information Management Policies, including:

- Data Protection Policy
- Security Incident and Personal Data Breach Policy
- Clear Desk Policy
- Home and Remote Working Policy
- Information Management Policy
- ICT Policy
- Home and Remote Working Policy

1.3 The Policy applies to all Members and employees of the Council, both permanent and temporary. It also applies to contractors, business partners and visitors, not employed by the council but engaged to work with or who have access to council information, (e.g. computer maintenance contractors) and in respect of any externally hosted computer systems.

1.4 The Policy applies to all locations from which council systems are accessed (including home use). Where there are links to enable non-council organisations to have access to council information, officers must confirm the security policies they operate meet the council's security requirements. A copy of any relevant third party security policy should be obtained and retained with the contract or agreement.

1.5 Suitable third party processing agreements must be in place before any third party is allowed access to personal information for which the Council is responsible.

2 Policy Compliance

2.1 Heads of Service should ensure all staff are aware of and understand the content of this policy.

2.2 If any user is found to have breached this policy, they could be subject to Fenland District Council's Disciplinary Policy & Procedure. Serious breaches of this policy could be regarded as gross misconduct.

3 Legal Aspects

3.1 Some aspects of information security are governed by legislation, the most notable UK Acts and European legislation are listed below:

- The Data Protection Act (2018)
- General Data Protection Regulation (GDPR)
- Copyright, Designs and Patents Act (1988)
- Computer Misuse Act (1990)

4 Responsibilities

4.1 Managers must:

- be aware of information or portable ICT equipment which is removed from the District Council offices for the purpose of site visits or home working and ensure staff are aware of the security requirements detailed in section 8, below
- ensure all staff, whether permanent or temporary, are instructed in their security responsibilities
- ensure staff using computer systems/media are trained in their use
- determine which individuals are given authority to access specific information systems. The level of access to specific systems should be on a job function need, irrespective of status
- ensure staff are unable to gain unauthorised access to council IT systems or manual data
- implement procedures to minimise the council's exposure to fraud, theft or disruption of its systems such as segregation of duties, dual control, peer review or staff rotation in critical susceptible areas
- ensure current documentation is maintained for all critical job functions to ensure continuity in the event of relevant staff being unavailable
- ensure that the relevant system administrators are advised immediately about staff changes affecting computer access (e.g. job function changes leaving business unit or organisation) so that passwords may be withdrawn or changed as appropriate

- ensure that all contractors undertaking work for the council have signed confidentiality (non-disclosure) undertakings

- ensure the council's Clear Desk Policy is adhered to, particularly in relation to confidential or personal information. The Clear Desk Policy can be found in Section 11 below.

- ensure information held is accurate, up to date, and retained, in line with council data retention and disposal

- ensure relevant staff are aware of and comply with any restrictions specific to their role or service area.

4.2 Members and Staff are responsible for:

- ensuring that no breaches of information security result from their actions

- reporting any breach, or suspected breach of security without delay.

- ensuring information they have access to remains secure. The level of security will depend on the sensitivity of the information and any risks which may arise from its loss.

- ensuring they are aware of and comply with any restrictions specific to their role or service area.

4.3 All staff should be aware of the confidentiality clauses in their contract of employment.

4.4 Advice and guidance on information security can be provided by the Data Protection Officer and, in relation to IT security, the IT Manager.

PART 1 - KEEPING INFORMATION SECURE

5 Data Protection by Design and Default

5.1 The General Data Protection Regulation (GDPR) requires that organisations put in place appropriate technical and organisational principles and safeguard individual rights. This is known as 'data protection by design and by default'. This means that we have to integrate data protection into our processing activities and business practices, from the design stage right through the lifecycle.

5.2 The council will, therefore, ensure that privacy and data protection is a key consideration in everything we do. As part of this we will:

- consider data protection issues as part of the design and implementation of systems, services, products and business practices;
- make data protection an essential component of the core functionality of our processing systems and services
- anticipate risks and privacy-invasive events before they occur and take steps to prevent harm to individuals
- only process the personal data that we need for our purpose(s) and that we only use the data for those purposes

5.3 Core privacy considerations should be incorporated into existing project management and risk management methodologies and policies to ensure:

- Potential problems are identified at an early stage
- Increased awareness of privacy and data protection
- Legal obligations are met and data breaches are minimised
- Actions are less likely to be privacy intrusive and have a negative impact on individuals

5.4 Data Protection Impact Assessments (DPIAs) are an integral part of taking a privacy by design approach. Guidance on undertaking a DPIA can be sought from the Data Protection Officer.

6 Data Breaches and Information Security Incidents

6.1 The council has a duty to ensure that all personal information is processed in compliance with the principles set out in the General Data Protection Regulation (GDPR). It is ultimately the responsibility of each Head of Service to ensure that their service areas comply with that duty and that suitable procedures are in place for staff to follow when dealing with personal information.

6.2 Staff should be aware of requirements in relation to identifying and reporting security incidents and personal data breaches.

7 Access control

7.1 Staff, Members and contractors should only access systems for which they are authorised. Under the Computer Misuse Act (1990) it is a criminal offence to attempt to gain access to computer information and systems for which they have no authorisation. All contracts of employment and conditions of contract for contractors should have a non-disclosure clause, which means that in the event of accidental unauthorised access to information (whether electronic or manual), the member of staff or contractor is prevented from disclosing information which they had no right to obtain.

7.2 Formal procedures will be used to control access to systems. An authorised manager/ Head of Service must authorise any system access requests for new staff. Access privileges will be modified/removed - as appropriate - when an individual changes job or leaves. Managers must ensure they advise IT of any changes requiring such modification/removal.

7.3 Staff, Members and contractors must comply with the council's in relation to passwords.

7.4 Line managers must ensure that passwords to local systems are removed or changed to deny access. This would apply where, for example, the system is externally hosted and not under the remit of IT

7.5 Where appropriate, staff working out notice are assigned to non-sensitive tasks or are appropriately monitored.

7.6 Particular attention should be paid to the return of items which may allow future access. These include personal identification devices, access cards, keys, passes, manuals & documents.

7.7 Once an employee has left, it can be impossible to enforce security disciplines, even though legal process. Many cases of unauthorised access into systems and premises can be traced back to information given out by former employees.

7.8 System administrators will delete or disable all identification codes and passwords relating to members of staff who leave the employment of the council. The employee's manager should ensure that all PC files of continuing interest to the business of the council are transferred to another user before the member of staff leaves

7.9 Managers must ensure that staff leaving the council's employment do not inappropriately wipe or delete information from hard disks. If the circumstances of leaving make this likely then access rights should be restricted to avoid damage to council information and equipment.

7.10 All visitors should have official identification issued by the council. If temporary passwords need to be issued to allow access to confidential systems these need to be disabled when the visitor has left. Visitors should not be afforded an opportunity to casually view computer screens or printed documents produced by any information system without authorisation.

7.11 There is a requirement for system administrators to have a procedure in place

for the secure control of contractors called upon to maintain and support computing equipment and software. The contractor may be on site or working remotely via a communications link. IT Services will advise on the most suitable control.

7.12 Physical security to all office areas is provided through the access control system. Staff should challenge strangers in the office areas without an ID badge. Never let someone you don't know or recognise to tailgate you through security doors.

8 Security of Equipment

8.1 Portable computers must have appropriate access protection, for example passwords and encryption, and must not be left unattended in public places.

8.2 Computer equipment is vulnerable to theft, loss or unauthorised access. Always secure laptops and handheld equipment when leaving an office unattended and lock equipment away when you are leaving the office.

8.3 Due to the high incidence of car thefts laptops or other portable equipment must **not** be left unattended in cars or taken into vulnerable areas.

8.4 Users of portable computing equipment are responsible for the security of the hardware and the information it holds at all times on or off council property. The equipment should only be used by the individual to which it is issued, be maintained and batteries recharged regularly.

8.5 Staff working from home must ensure appropriate security is in place to protect council equipment or information. This will include physical security measures to prevent unauthorised entry to the home and ensuring council equipment and information is kept out of sight.

8.6 Council issued equipment must not be used by non-council staff.

8.7 All of the policy statements regarding the use of software and games apply equally to users of portable equipment belonging to the council.

8.8 Users of this equipment must pay particular attention to the protection of personal data and commercially sensitive data.

8.9 Users of portable equipment away from council premises should check their car and home insurance policies for their level of cover in the event of equipment being stolen or damaged and take appropriate precautions to minimise risk of theft or damage.

8.10 Staff and Members who use portable computers belonging to the council must use them solely for business purposes otherwise there may be a personal tax/National Insurance liability.

9 Payment Card Industry (PCI) Compliance

9.1 The Council is currently PCI DSS compliant, the Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to ensure that all companies that process, store or transmit credit or debit card information

maintain a secure environment.

9.2 Failure to comply with these standards could lead to fines or even the removal of the Councils ability to accept card payments.

9.3 Those users who have access to any part of the Councils Cash Receipting systems whereby they are taking payments either in person or over the phone should only enter Card numbers into the relevant Capita payment screens and **under no circumstances** should Card Holder data such as Card Numbers be written down or copied by anybody as this would breach our PCI compliance.

10 Security and Storage of Information

10.1 All information, whether electronic or manual, must be stored in a secure manner, appropriate to its sensitivity. It is for each service area to determine the sensitivity of the information held and the relevant storage appropriate to that information. Suitable storage and security will include:

- Paper files stored in lockable cupboards or drawers
- Laptops stored in lockable cupboards or drawers
- Electronic files password protected or encrypted
- Restricted access to ICT systems
- Computer screens to be 'locked' whenever staff leave their desk
- Removable media to be kept in lockable cupboards or drawers and information deleted when no longer required
- Paper files removed from the office (for site visits or when working from home) to be kept secure at all times and not left in plain sight in unattended vehicles or premises
- Laptops must **not** be left in unattended vehicles
- It is advisable that paper files containing personal or sensitive data are kept separate from laptops, particularly when working from home
- At no time should sensitive, confidential or personal information be stored on a portable unit's hard drive. Access to this type of information must always be through the council's network.
- To preserve the integrity of data, frequent transfers must be maintained between portable units and the main council computer system.
- Staff should be aware of the position of their computer screens and take all necessary steps to prevent members of the public or visitors from being able to view the content of computers or hard copy information

11 Clear Desk Policy

11.1 Employees are required to clear working documents, open files, and other paperwork from their desks, working surfaces and shelves at the end of each working day and to place them securely into desk drawers and cupboards as appropriate.

11.2 Although security measures are in place to ensure only authorised access to office areas, employees should ensure that documents, particularly of a confidential nature are not left lying around.

11.3 Employees must ensure that documents are carefully stored. When properly implemented, this clear desk policy also improves efficiency as documents can be retrieved more easily.

12 Posting or Emailing Information

12.1 If information is particularly sensitive or confidential the most secure method of transmission must be selected. The following procedures should be adopted as appropriate, depending on the sensitivity of the information.

12.2 Please consider the risk of harm or distress that could be caused to the customer if the information was lost or sent to another person, then look at the most appropriate way of sending the information to the recipient.

12.3 It is important that only the minimum amount of personal or sensitive information is sent, by whichever method is chosen.

12.4 Sending information by email:

- Carefully check the recipient's email address before pressing send – this is particularly important where the 'to' field autocompletes
- If personal or sensitive information is regularly sent via email, consider disabling the auto complete function and regularly empty the auto complete list. Both of these options can be found in Outlook under 'file', 'options' and 'mail'
- Take care when replying 'to all' – do you know who all recipients are and do they all need to receive the information you are sending
- If emailing sensitive information, password protect any attachments. Use a different method to communicate the password eg telephone call, messenger or text
- Person identifiable data files **must not** be sent via email to a user's personal mail box. Staff working from home should only access information via the council's network.

12.5 Sending information by post:

- Check that the address is correct

- Ensure only the relevant information is in the envelope and that someone else's letter hasn't been included in error

- If the information is particularly sensitive or confidential, discuss the most secure method of delivery with the Post room, this could be by Special Delivery or even courier.

12.6 Printing and Photocopying:

- All printing must be via the MFP printers

- Consideration must be given to using the Print Room for large print runs, especially where personal information is concerned

- When printing or photocopying multiple documents, ensure you separate them when you return to your desk

- If the copier jams please remove all documents – if the copier remains jammed report it, but leave your contact details on the copier so that once it has been fixed any remaining copying can be returned to you. If possible, cancel your print run

- Make sure your entire document has copied or printed – check that the copier has not run out of paper. This is particularly important when copying or printing large documents. Please bear in mind the printer will sometimes pause in the middle of a large print run

- Do not leave the printer unattended when you're using it – someone else may come along and pick up your printing by mistake

13 Redacting

13.1 If it is necessary to redact information, either before sending it out or posting it onto the website, ensure a suitable and permanent redaction method is used

13.2 It is not advisable to change the colour of text (eg white text on a white background) or use text boxes to cover text as these can be removed from electronic documents. However, if this is the only option, once redacted the document should be printed and then scanned as a PDF before being sent.

13.4 Redaction can be carried out by Member Services using Adobe Professional. Please contact Member Services for further information.

14 Sharing and Disclosing Information

14.1 When disclosing personal or sensitive information to customers, particularly over the phone or in person, ensure you verify their identity. Service areas dealing with customers on a daily basis should have suitable security questions which must always be used. If in doubt ask for suitable ID or offer to post the information (to the contact details you have on file)

14.2 If a request for disclosure of information is received from a third party, you must:

- Obtain written consent from the customer that they are acting on their behalf
- verify their identity, particularly if they request information via the telephone or in person. It is preferable to telephone the person back, using a recognised telephone number for their organisation (for example 101 for the Police). Do not take their mobile number and use that.

14.3 In all circumstances, you must ensure you are legally able to share the information being requested and only share the minimum amount of information necessary.

15 Retention and Disposal of Information

15.1 Information must only be retained for as long as it is needed for business purposes, or in accordance with any statutory retention period

15.2 Staff should refer to the council's Data Retention Policy for further information. The Schedule sets out the type of information held in service areas, together with statutory or agreed retention periods. Please contact the Data Protection Officer for further advice on retention

15.3 When disposing of information please ensure the most appropriate method is used. Paper files containing personal or sensitive information must be disposed of in the confidential waste bins. Electronic information must be permanently destroyed

15.4 When purchasing new computer systems or software, please consider requirements for the retention and disposal of information and ensure these are included at the scoping stage

16 Vacating Premises or Disposing of Equipment

16.1 It is important that a process is in place to ensure all council information is removed from premises should they be vacated and from equipment before it is disposed of. Equipment includes cupboards and filing cabinets as well as computers or other electronic devices.

16.2 The disposal of computers or other electronic devices should be discussed with the IT department.

16.3 If the council vacates any of its premises, the manager of the service area occupying the premises must undertake appropriate checks of all areas, including locked rooms, basements and other storage areas, to ensure all council information is removed. Such checks should be documented, dated and signed.

16.4 If information is bagged for disposal (whether confidential or not), this must be

removed before the building is vacated.

16.5 Cupboards and filing cabinets must be checked before their disposal to ensure they contain no documents or papers. If a cupboard or cabinet is locked and no key is available, Building Facilities should be asked to open it in order that it can be checked.