# EAST CAMBRIDGESHIRE DISTRICT COUNCIL

# INFORMATON SECURITY POLICY

| | |
|---|---|
| Title | Information Security Policy |
| Owner | ICT Manager |
| Issue date | January 2020 |
| Version Number | V1.0 |
| Next revision due | January 2023 |

## Contents

# 1 Introduction

1.1 All information held by the Council, in all formats, represents an extremely valuable asset, however without it our jobs would be impossible to do.

Information is precious and, therefore, must be used and stored in a secure manner. We have identified information management and security as one of our key risks. Information Security is everyone's responsibility and this policy will provide guidance covering all aspects of processing information.

1.2 The Policy must be read in conjunction with other information management and IT Policies, Code of Practice and guidance documents, including but not limited to;

- Data Protection Guidance
- Data Breach Guidance
- Remote Working Code of Practice
- Social Media Guidance
- ICT Equipment, Internet and Email Acceptable Use Policy
- Data Retention and Disposal Guidelines
- ICT Password Policy
- ICT Starter Leavers Procedure

1.3 The Policy applies to all Members, employees of the Council, and employees of all entities owned by the Council. 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 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.

1.6 The policy applies throughout the lifecycle of the information from creation, storage and use, to disposal. It applies to all information including;

- Information stored electronically in databases or applications e.g. email;
- Information stored on computers, laptops, tablets, mobile phones or removable media such as hard disks, CD/DVD's, memory sticks and other similar media;

- Information stored on networks;
- Information sent by fax or other communications method;
- All paper records;
- Microfiche, visual and photographic materials including CCTV
- Spoken, including face-to-face, voicemail and recorded conversation

## 2.0 Definition of Information Security

2.1 Information security means safeguarding information from unauthorised access or modification to ensure its:

- **Confidentiality** – ensuring the information is accessible only to those authorised to have access;
- **Integrity** – safeguarding the accuracy and completeness of information by protecting against unauthorised modification;
- **Availability** – ensuring that authorised users have access to information and associated assets when required.

## 3.0 Policy Compliance

3.1 Service Leads should ensure all staff are aware of and understand the content of this policy.

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

## 4.0 Legal and Regulatory Requirements

4.1 Users of the Council's information assets will be required to abide by UK and European Legislation relevant to security including;

- Data Protection Act 2018
- The General Data Protection Regulation (GDPR)
- Computer Misuse Act 1990
- Privacy and Electronic Communications Regulations 2003
- Copyright, Designs and Patents Act 1988
- Freedom of Information Act 2000
- Payment Card Industry Data Security Standards (PCI DSS)
- Users should seek guidance about the legal constraints of using information in their work and the Council will provide appropriate guidance and training to its staff.

## 5.0 Roles and Responsibilities

5.1 The Council's Senior Information Risk Officer (SIRO) has responsibility for managing information risk on behalf of the Chief Executive and the Council's Management Team, setting strategic direction and ensuring policies and processors are in place for sage management of information.

5.2 Service Leads and Line Managers must:

5.2.1 ensure all staff, whether permanent or temporary, are instructed in their security responsibilities

5.2.2 ensure staff using computer systems/media are trained in their use

5.2.3 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

5.2.4 ensure staff are unable to gain unauthorised access to council IT systems or manual data

5.2.5 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.

5.2.6 ensure current documentation is maintained for all critical job functions to ensure continuity in the event of relevant staff being unavailable

5.2.7 ensure that the relevant system administrators are advised immediately about staff changes affecting computer access (e.g. job function changes or leaving the Council or its Trading Companies) so that passwords may be changed or accounts deactivated and/or amend data access rights.

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

5.2.9 be aware of information or portable ICT equipment which is removed from The Council Offices for the purpose of site visits or home working and ensure staff are aware of the security requirements detailed in Section 9.

5.2.10 ensure relevant staff are aware of and comply with any restrictions specific to their role or service area. This would include Data Sharing Agreements to which the Council is a signatory

5.3 Members and Staff are responsible for:

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

5.3.2 reporting any breach, or suspected breach of security to the Council's Information Officer without delay. Further details can be found in the Data Protection Guidance for Staff document (found on the East Cambridgeshire District Council's Intranet - Data Protection Pages https://intranet.eastcambs.gov.uk/policies/data-protection)

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

5.3.4 ensuring they are aware of and comply with any restrictions specific to their role or service area. This would include, for example, Memoranda of Understanding with Government Departments and Data sharing Agreements to which the council is a signatory.

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

5.5 Advice and guidance on information security can be provided by the Information Officer (Legal) and, in relation to IT Security, the ICT Manager.

## 6.0 Keeping Data Secure

6.1 Data Protection by Design and Default

6.1.1 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 Default'. It means we have to integrate data protection into our processing activities and business practices from the design stage right through the lifecycle.

6.1.2 The Council will 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 of 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

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

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

6.3 All paperwork particularly those that include sensitive and/or personal identifiable information should be locked away when not in use and at the end of each day.

## 7.0 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 All new starters will only be given controlled access to applications/systems and data file areas as provided by line managers on the IT New Starter Form. Additions or changes to the access privileges to any application/system and data file areas must be made using the ICT Helpdesk and will only be actioned following authorisation from the employee's line manager or Director.

7.3 The ICT Team must be informed by HR or by an employee's Line Manager or Director before the last working day of employment for any employee leaving the Council. The ICT Team will remove access rights to the employees Network Account.

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

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

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

7.7 Staff, Members and contractors must comply with the council's Password Policy.

7.8 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 and documents.

7.9 Managers must ensure that staff leaving the council's employment do not inappropriately wipe or delete information from devices. 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 Physical security to the building with the exception of the reception is provided through access control. Staff and Members should challenge anyone they do not recognise in the office areas. Never let someone you don't know or recognise to tailgate you through security doors.

## 8.0 Security of Equipment

8.1 Portable devices with the ability to store data must have appropriate access protection, for example passwords and encryption.

8.2 Portable devices must not be left unattended in public places.

8.3 Computer equipment is vulnerable to theft, loss or unauthorised access. Any authorised user of council portable devices should secure laptops and handheld equipment with the equipment being locked away when they leave the office.

8.4 Portable devices must be kept out of site when travelling in a vehicle and should always be locked away in the glove box or similar or the boot of the vehicle.

8.5 Users of portable devices 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.

8.6 Users 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 property and ensuring council equipment and information is kept out of sight.

8.7 Council issued equipment must not be used by non-council staff and members.

## 9.0 Payment Card Industry (PCI) Compliance

9.1 The Council is currently Payment Card Industry Data Security Standard (PCI DSS) compliant. This 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 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.

## 10.0 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 the information. Suitable storage and security includes:

- Paper files stored in lockable cupboards or drawers
- Portable devices 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 (for example, CD, DVDs and USB pens/sticks/drives) should be kept in lockable cupboards or drawers and information deleted or media destroyed (e.g. CD) when no longer required. Removable media should not be plugged into Council’s devices unless authorised by the ICT Team .
- 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
- Portable Devices should not be left in unattended vehicles
- It is advisable that paper files containing personal or sensitive data are kept separate from Portal Devices, particularly when working from home
- At no time should sensitive, confidential or personal information be stored on a portable device’s hard drive. Access to this type of information must always be through the council’s network.
- 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 displayed on the screens.

## 11.0 Posting, Emailing and Copying Information

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

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

11.3 Sending information by email:

11.3.1 Carefully check the recipient’s email address before pressing send – this is particularly important where the ‘to’ field autocompletes.

11.3.2 If personal or sensitive information is regularly sent via email, consideration should be given to disabling the auto complete function and regularly empty the auto complete list. Both options can be found in Outlook under ‘file’, ‘options’ and ‘mail’.

11.3.3 Staff and Members should take care when replying 'to all' – do you know who all recipients are and do they all need to receive the information being sent.

11.3.4 If emailing sensitive information, password protect any attachments. Use a different method to communicate the password e.g. telephone call or text

11.4 Sending information by post:

11.4.1 Check the recipient's address is correct.

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

11.4.3 If the information is particularly sensitive or confidential send using the most secure method of delivery, this could be Special Delivery or Courier.

11.5 Printing and Photocopying:

11.5.1 When printing or photocopying multiple documents, Staff and Members should ensure the documents are separated.

11.5.2 Make sure your entire document has copied or printed – check that the copier/printer has not run of paper. This is particularly important when copying or printing large documents.

11.5.3 Do not leave the printer unattended – someone else may come along and pick up the printing by mistake.

11.5.4 Consideration should be given to printing of sensitive data and should be printed using the MFD printers, where possible due to the more secure nature of the printer (authentication by user card)

## 12.0 Redacting

12.1 Any third party data should be redacted either before sending it out or posting it onto the website. A suitable and permanent redaction method should be used.

12.2 The use of black marker pen is **not** a suitable method of redaction.

12.3 Changing the colour of text (e.g. white text on a white background) or using text boxes to cover text are not suitable redaction methods, as these can be removed from electronic documents. If guidance is needed for redacting documents, please contact the ICT Team.

## 13.0 Sharing and Disclosing Information

13.1 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 on file).

13.2 If a request for disclosure of information is received the request must be referred to the Information Officer (Legal)

## 14.0 Retention and Disposal of Information

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

14.2 Staff should refer to the Council's Retention and Disposal Guidelines for further information. The schedule sets out the type of information held in service areas, together with statutory or agreed retention periods. Contact the Information Officer (Legal) for further advice on retention.

14.3 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/bags. Electronic information must be permanently destroyed.

14.4 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.

14.5 When a member of staff leaves, their electronic stored data (Email mailbox, "Private" file storage on the network) will be archived and stored for 3 years. The electronic data may be accessed by the leaver's Line Manager, Service Lead or Director and any electronic data may be copied/moved out of the storage archive if deemed necessary for business purposes. The electronic data in the storage archive will be destroyed in lines with the Council's retention and Disposal Guidelines after the 3 year period.

## 15.0 Vacating Premises or Disposing of Equipment

15.1 All Council information should be removed from the premises should they be vacated and from equipment before it is disposed of. Equipment includes cupboards and filling cabinets as well as computers or other electronic devices.

15.2 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.

15.3 If information is bagged for disposal (whether confidential or not), this must be removed before the building is vacated.

15.4 Cupboards and filing cabinets must be checked before their disposal to ensure they contain no documents or papers.

15.5 All ICT equipment should be disposed of by the ICT Team. The ICT Team will arrange the disposal of the equipment through a company with the necessary credentials for that type of equipment e.g. hard drive shredded

## 16.0 Cloud Storage Solutions

16.1 The use of cloud storage solutions (Dropbox, Onedrive Personal, iCloud etc.) for the transfer of council information should not be used without prior authorisation from both the Legal and ICT Teams.

## 17 Systems Development

17.1 All system developments must include security issues in their consideration of new developments, seeking guidance from the IT Team where appropriate.

17.2 Data Privacy Impact Assessments (DPIAs) should be carried out prior to purchase of any new system which will be used for storing and accessing personal information, please see the Information Officer (Legal) prior to any new systems or technologies being implemented.

## 18 Network Security

18.1 The Council will engage a third-party specialist to routinely review network security.

## 19 Risks from Viruses and other malicious software

19.1 Viruses (including malware and zero day threats) are one of the greatest threats to the council’s computer systems. PC viruses become easier to avoid if staff and members are aware of the risks with unlicensed software or bringing data/software from outside the council. Anti-virus measures reduce the risks of damage to the network.

19.2 ICT centrally maintain and update the currency of the virus definition files on servers, but users are responsible for checking that virus updates are automatically occurring on all desktop machines. Advice and support is available from the ICT Team if any remedial action is necessary. Any suspected virus attack must be report by the ICT Helpdesk.

19.3 Ransomware is becoming more common and is a serious threat to data stored by the council. A device, system or network attacked by ransomware may have all files it has access to encrypted and in some cases may have the data stolen by malicious attacks. Ransomware, and many common viruses, are often distributed via malicious email or malicious websites. Only click links and download/open attachments from trusted sources and only when you expect the item(s). Do not open or download a file if you are not sure.

## 20 Cyber Security

20.1 Cyber security and cybercrime are increasing risks that, if left unchecked, could disrupt the day to day operations of the Council, the delivery of local public services and ultimately have the potential to compromise national security.

20.2 Regular cyber security training will be provided to all staff and members.

## 21 Access to Secure Areas

21.1 The Council's local network equipment and servers will be located in secure areas and where appropriate within locked cabinets.

21.2 Unrestricted access to the central computer facilities will be confined to designated staff whose job function requires access to that particular area/equipment.

21.3 Restricted access may be given to other staff where there is a specific job function need for such access.

21.4 Authenticated representatives of third party support agencies will only be given access through specific authorisation.

## 22 Security of Third Party Access

22.1 No external agency will be given access to any of the council's networks unless that body has been formally authorised to have access.

22.2 All external agencies will be required to sign security and confidentiality agreements with the council.

22.3 All external agencies processing personal information on the council's behalf (including via a hosted IT System) will be required to sign a third party processing agreement.

22.4 The council will control all external agencies access to its systems by enabling/disabling connections for each approved access requirement.

22.5 The council will put in place adequate procedures to ensure the protection of all information being sent to external systems. In doing so, it will make no assumptions as to the quality of security used by any third party but will request confirmation of levels of security maintained by those third parties. Where levels of security are found to be inadequate, alternative ways of sending data will be used.

22.6 All third parties and any outsourced operations will be liable to the same level of confidentiality as council staff and members.

## 23 Data backup

23.1 Data should be held on a network directory where possible, to ensure routine backup processes capture the data. Information must not be held on a device's local storage without the prior approval of the ICT Manager.

23.2 Data should be protected by clearly defined and controlled back-up procedures which will generate data for archiving and contingency recovery purposes.

23.3 ICT should produce written backup instructions for IT Systems under their management. Procedures should be in place to recover to a useable point after restart of this back-up.

23.4 Archived and recovery data should be accorded the same security as live data and should be held separately preferably at an off-site location. Archived data is information which is no longer in current use, but may be required in the future, for example, for legal reason or audit purposes. The council's Retention and Disposal Guidelines must be followed in determining whether data should be archived.

23.5 Recovery data should be sufficient to provide an adequate level of service and recovery time in the event of an emergency and should be regularly tested as determined by the Disaster Recovery Document.

23.6 Recovery data should be used only with the formal permission of the data owner, the relevant Service Lead/Director or as defined in the contingency plan for the system.

23.7 If live data is corrupted, any relevant software, hardware and communications facilities should be checked before using the back-up data. This aims to ensure that the back-up is not corrupted in addition to the live data. An engineer (software or hardware) should check the relevant equipment or software using his/her own test data.

## 24 Software

24.1 All users should ensure that they only use licensed copies of commercial software. It is a criminal offence to make/use unauthorised copies of commercial software and offender are liable to disciplinary action. Each user should ensure that a copy of each licence for commercial software is held.

24.2 The loading and use of unlicensed software on council computing equipment is **NOT** allowed. All staff and member must comply with the Copyright, Designs and Patents Act (1988). This states that it is illegal to copy and use software without the copyright owner's consent or the appropriate licence to prove the software was legally acquired. The council monitors the installation and use of software by means of regular software audits; any breaches or software copyright may result in personal litigation by the software author or distributor and may be the basis for disciplinary action under the councils Disciplinary Policy and Procedures.

24.3 The council will only permit authorised software to be installed on its IT equipment. Approval will be via ICT Team. Any requests for software to be installed should be made by the ICT Helpdesk.

24.4 Where the council recognises the need for specific specialised PC products, such products should be registered with ICT and be fully licensed.

24.5 Software packages must comply with and not compromise council security standards.

24.6 Computers owned by the council are only to be used for the work of the council. The copying of leisure software on to computing equipment owned by the council is not allowed. Copying of leisure software may result in disciplinary actions under the councils Disciplinary Policy and Procedures. Computer leisure software is one of the main sources of software corruption and viruses which may lead to the destruction of complete systems and the data contained on them.

24.7 Education software for training and instruction should be authorised, properly purchased, virus checked and installed by ICT Team. Where a software package includes 'games' (for example, to enable the user to practise their keyboard skills), then this will be allowed as long as it does not represent a threat to the security of the system.

24.8 The council seeks to minimise the risks of computer viruses through education, good practice/procedures and anti-virus software position in the most vulnerable areas. Users should report any viruses detected/suspected on their machine **immediately** to ICT via the ICT Helpdesk.

24.9 Users must be aware of the risks of viruses from email and the internet. If in doubt any data received users should contact the ICT Team for advice.

## 25 Timeout and Account Lockout

25.1 Inactive computers should be set to time out after a pre-set period of inactivity. The time-out facility should clear the screen.

25.2 Users must 'lock' their computers, if leaving them unattended. For high risk applications, connection time restriction should be considered. Limiting the period during which the computer has access to the IT Services reduces the window of opportunity for unauthorised access.

25.3 Users computer accounts must adhere to PCI requirements (see Section 9). At time of writing this requires passwords to be reset every 90 days and the account to be locked after 3 incorrect login attempts.

## 26 Document Review

26.1 The policy will be reviewed every 3 years or sooner if deemed necessary (for example introduction of new legislation).