Agenda Item No:	10	
Committee:	Corporate Governance Committee	
Date:	05 November 2019	
Report Title:	Data Protection - Policy Reports	

1 Purpose / Summary

To provide the Corporate Governance Committee with an update regarding key policies including a revised Data Protection Policy, Information Security Policy and Reporting Personal Data Breaches Policy and Procedure, which collectively and proactively demonstrate the Council's commitment to protecting individuals' privacy whilst also fulfilling our obligations under data protection legislation.

2 Key issues

- In order to provide services to local residents and businesses, the Council collects, uses and shares considerable amounts of personal data. Personal data refers to any information that can identify a living individual, such as their name, email address, address, health conditions or CCTV footage of them.
- The European Union-wide General Data Protection Regulation (GDPR) and the Data Protection Act 2018 set requirements on how organisations, including councils, can process personal data. Through six principles, the legislation establishes that personal data shall be:
    - processed lawfully, fairly and in a transparent manner
    - collected and processed for specified, explicit and legitimate purposes
    - adequate, relevant and limited to what is necessary for those purposes
    - kept accurate, and where necessary, up to date
    - kept in a form that identifies the person for no longer than is necessary
    - processed in a manner ensuring its security.
- In order to uphold these principles, the revised Data Protection Policy (contained within Appendix 1 of this report) reflects the legislative changes in addition to reflecting the greater emphasis on proactive compliance and data subject rights.
- 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.
- The Information Security Policy (contained within appendix 2 of this report) outlines our commitment to ensuring information is stored securely and that those considerations are a fundamental consideration therefore achieving ‘Data Protection by Design and Default’.
- Naturally Fenland District Council will seek to avoid personal data breaches, however it is recognised that there are risks associated with the collection, use, transmission and storage of personal data in order to conduct official council business. The Council recognises that a personal data breach, if not addressed in an appropriate and timely manner, can result in physical, material or non-material damage to individuals.
- The definition of a “personal data breach” is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
- The aim of the Reporting Personal Data Breaches Policy and procedure (contained within appendix 3 of this report) is to ensure that the Council reacts appropriately to any actual or suspected personal data breaches in accordance with GDPR, whilst also proactively identifying area for improvement.

3 Recommendations

- For Corporate Governance Committee to agree the revised Data Protection Policy as outlined in Appendix 1, which applies to all staff and elected members
- To agree the Data Security Policy as outlined in Appendix 2, which applies to all staff and elected members
- To agree the Reporting Personal Data Breaches Policy and Procedure as outlined in Appendix 3, which applies to all staff and elected members.

Wards Affected	All
Forward Plan Reference	
Portfolio Holder(s)	Councillor Chris Boden, Leader and Portfolio Holder - Quality Org.
Report Originator(s)	Anna Goodall - Data Protection Officer
Contact Officer(s)	Peter Catchpole - Corporate Director petercatchpole@fenland.gov.uk Anna Goodall, Data Protection Officer agoodall@fenland.gov.uk 01354 622357
Background Paper(s)	

Fenland District Council

APPENDIX 1

Data Protection Policy

September 2019

Document information

Version Number	V01	
Document Status (Draft/Final)	Final	
Effective from date	September 2019	
Review date	September 2020	
Reason for document	Alignment of policies and compliance with updated Data Protection Act and General Data Protection Regulation	
Linked documentation	1. Information Security Policy 2. Impact Assessment Policy 3. Personal Data Breach Policy	
Author	Name	Anna Goodall
	Job Title	Head of Governance & Legal
	Team	Governance
	Contact	agoodall@fenland.gov.uk

Contents

1. Introduction

1.1 Fenland District Council supports the objectives of the General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA) and seeks to ensure compliance with this data protection legislation.

1.2 The processing of data by the Council is essential to services and functions, and will often involve the use of personal and/or 'special category' personal data. Compliance with the data protection legislation will ensure that such processing is carried out fairly and lawfully.

1.3 The GDPR and the Human Rights Act (1998) (HRA) Article 8, make it clear that the processing of personal data must respect the rights and freedoms of the data subject (individual), but at the same time be adequate enough for the Council to function effectively.

1.4 This policy should not be read in isolation and regard should be given to the Council's Information Security Policy.

2. Purpose

2.1 The purpose of this policy is to ensure that the provisions of the GDPR and DPA are adhered to whilst protecting the rights and privacy of living individuals**;** ensuring their personal data is not processed without their knowledge.

2.2 In particular this policy will:

- Assist the Council to comply with all requirements of the GDPR and DPA.
- Ensure that personal data is readily available on request and that requests from data subjects are dealt with in a timely manner.
- Ensure adequate consideration is given to whether or not personal information should be disclosed.
- Ensure increased awareness of data subjects to the amount of personal data processed and stored by the Council about them and advise them of their rights under the data protection legislation.

2.3 The Council will endeavour to promote greater openness, provide increased transparency of data processing and build public trust and confidence in the way that the Council manages information about its customers.

3. Aims

3.1 This policy sets out the Council's commitment to upholding the data protection principles set out in the GDPR and managing information held fairly and lawfully. It seeks to strike an appropriate balance between the Council's need to make use of personal information in order to manage their services efficiently and effectively and respect for the privacy of individuals.

3.2 To assist staff in meeting their statutory obligations under the GDPR and DPA and provide a guide to the public on the Council's obligations with regard to the processing of their personal data.

4. Council statement on data protection requirements

4.1 This policy applies to the acquisition and processing of all personal data within the Council and sets out how the Council will ensure that individual rights and freedoms are protected.

- The Council will comply with Article 8 of the HRA in respect of the processing of personal data.
- The Council, as the Data Controller, will make individuals aware of the purpose(s) it is processing their personal data for and will seek consent where appropriate.
- 'Consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
- The Council will provide general information to the public about their statutory rights under the GDPR and DPA on our website.
- The Council will hold the minimum amount of personal data necessary to carry out its functions, and every effort will be made to ensure the accuracy and relevance of data processed.
- The Council will keep all electronic and manual records in accordance with its Data Retention Policy.
- The personal data the Council holds will be kept in accordance with the six principles of the GDPR and in line with the Council's data retention policy

- Periodically a risk assessment will be undertaken, via audit reviews, for all data processing, and when inadequate controls are identified, technical and organisational security measures will be taken, appropriate to the level of risk identified.

- Personal data will only be used for the direct promotion or marketing of goods or services with the explicit consent of an individual.

- Data sharing and data matching with external agencies will only be carried out under a written contract setting out the scope and limits of the data agreement. This should be in line with the Council's Data Sharing Policy.

- Elected Members and staff will be trained to an appropriate level in the use and supervision of personal data.

- Breaches of this policy may be subject to action under the Council's disciplinary procedure.

4.2 The Council will abide by the six data protection principles as detailed below: Personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency').

- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1) not be considered incompatible with the initial purposes ('purpose limitation').

- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').

- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy').

- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational

measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation').

- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

5. Roles and responsibilities

5.1 The Council's Corporate Management Team is responsible for approving this policy for managing compliance with the GDPR and DPA.

5.2 Overall responsibility for the GDPR and DPA will rest with the Chief Executive in consultation with the Data Protection Officer.

5.3 The Council's Data Protection Officer is responsible for the provision of advice, guidance and training regarding data protection legislation and will be responsible for keeping this document up to date.

5.4 All employees of the Council will be responsible for ensuring that Subject Access Requests are dealt with in accordance with this policy and that personal data is processed appropriately. This includes ensuring that personal data supplied to the Council is accurate, up-to-date and held securely.

5.5 Heads of Service will be responsible for ensuring operational compliance with this policy within their own departments and for becoming involved in consultations with the Data Protection Officer when applicable.

5.6 Internal Audit will undertake reviews to assess the procedures and policies in place that relate to data protection.

6. Information requests

6.1 Requests from data subjects for copies of personal data the Council holds about them (Subject Access Requests) can be made in writing or verbally. This includes requests transmitted by electronic means, providing they are received in a legible form and are capable of being used for subsequent reference.

6.2 If a person is unable to articulate their request in writing we will provide advice to assist them in formulating their request.

6.3 If the information sought is not described in a way that would enable the council to identify and locate the requested material, or the request is ambiguous, the Council will seek additional clarification.

6.4 The Council will not provide assistance to an applicant who is not the data subject, unless it is confirmed that the explicit consent of the data subject has been obtained for a third party to request the data subject's personal data.

7. Prompt replies to requests

7.1 The Council is committed to dealing with requests for information promptly and no later than the statutory guideline of one calendar month.

7.2 The Council would not expect every application for information to take one calendar month and will endeavour, where possible, to provide the requested information at the earliest opportunity from the date of the request.

7.3 However, if the Council considers the request to be complex, it may extend the time by up to two extra calendar months.

7.4 In this instance the Council will notify the applicant in writing that the SAR requires further time and will provide an estimate of a 'reasonable time' by which they expect a response to be made.

7.5 These estimates shall be realistic and reasonable taking into account the circumstances of each particular case.

8. Data subject rights

8.1 Subject to some legal exceptions, individuals will have the rights below.

- Right to request a copy of any information we hold about you
- Right to rectification (if inaccurate data is held)
- Right to erasure ('right to be forgotten') in certain circumstances
- Right to restriction of processing in certain circumstances
- Right to data portability (personal data transferred from one data controller to another)
- Right to object (to profiling, direct marketing, automated decision-making)

9. Exempting information from non-disclosure

9.1 The GDPR is designed to prevent access by third parties to a data subject's personal data. However, under the DPA there are circumstances which allow disclosure of a data subject's personal data to a third party, or for it to be used in a situation that would normally be considered to breach the GDPR.

9.2 Exemptions from the non-disclosure of personal data are given below. This list is not exhaustive.

- Crime and taxation: general

    a) the prevention and detection of crime
    b) the apprehension or prosecution of offenders, or
    c) the assessment or collection of any tax or duty or of any imposition of a similar nature

- Crime and taxation: risk assessment systems
- Immigration
- Information required to be disclosed by law etc. or in connection with legal proceedings

9.3 The Council will only use these exemptions where it is in the public interest to do so, i.e. prevention of crime, or where the functioning of the Council requires the processing of personal information to be exempt so that it can provide statutory services to members of the public.

10. Refusal of subject access requests

10.1 The Council will not supply information to a data subject if:

- We are not satisfied with the identity of the data subject
- Compliance with the request will inadvertently disclose personal information relating to another individual without their consent
- The applicant has recently requested the same or similar information

10.2 The Council considers that when a valid reason, which is both robust and legally defendable, exists for refusing the disclosure of information to either the data subject or a third party, the information should be withheld.

10.3 When information is withheld, full explanations of the reasoning behind the refusal must be provided to the applicant. This explanation must also include the details of how the applicant can complain about the Council's decision.

10.4 All requests for personal data made by the data subject will be dealt with under Chapter 3 - Rights of the Data Subject section of the GDPR, not the Freedom of Information Act 2000.

11. Appeals and complaints

11.1 Where an applicant is dissatisfied with the level of service they have received, they are entitled to complain about the actions of the Council through the internal appeals procedure. All complaints should be forwarded to:

Member Services
Fenland District Council, County Road, March, Cambs PE15 8NQ

E-mail: foi@fenland.gov.uk

11.2 The applicant will receive a response to their correspondence within twenty working days. If the applicant remains dissatisfied with the Council's reply, they have the option of taking their complaint to the Information Commissioner (at the address below) who will independently adjudicate each case and make a final decision.

Information Commissioner's Office
Wycliffe House,
Water Lane
Wilmslow
Cheshire
SK9 5AF

Appendix 1

Interpretation of Terms

1. 'Personal data' means any information relating to an identified or identifiable living individual ('data subject')

‘Identifiable living individual’ means a living individual who can be identified, directly or indirectly, in particular by reference to

a) an identifier such as a name, an identification number, location data or an online identifier, or
b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

2. ‘Special category (sensitive) personal data’ means:

- Racial or ethnic origin
- Political opinions
- Religious/philosophical beliefs
- Trade union
- Processing of biometric/genetic data to identify someone
- Health
- Sex life or sexual orientation

3. ‘Processing’, in relation to personal data, means an operation or set of operations which is performed on personal data or on sets of personal data, such as:

a) collection, recording, organisation, structuring, storage
b) adaptation or alteration
c) retrieval, consultation, use
d) disclosure by transmission, dissemination or otherwise making available
e) alignment or combination, or
f) restriction, erasure or destruction.

4. ‘Data subject’ means the identified or identifiable living individual to whom personal data relates.

5. ‘Controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

6. ‘Processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

7. ‘Filing system’ means any structured set of personal data which is accessible according to specific criteria, whether held by automated means or manually and whether centralised, decentralised or dispersed on a functional or geographical basis.

8. ‘Consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

APPENDIX 2

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. Further details can be found on the following link:

  https://www.fenland.gov.uk/intranet/memberservices

- 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 and the assessment form can found on the Intranet on the link below:

https://www.fenland.gov.uk/intranet/memberservices

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 ICT-related policies in relation to passwords. Further information can be found on the Intranet:

https://www.fenland.gov.uk/intranet/ict

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 Council's ability to accept card payments.

9.3 Those users who have access to any part of the Council's 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 e.g. 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 are 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 (e.g. 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.

13.3 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.

14.4 Further information on Disclosure of Information under DPA 2018 can be found on the link below:

https://www.fenland.gov.uk/intranet/memberservices

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.

Fenland District Council

APPENDIX 3

Reporting Personal Data Breaches

Policy and Procedures

1. Policy Statement

Fenland District Council will seek to avoid personal data breaches. The Council recognises that a personal data breach, if not addressed in an appropriate and timely manner, can result in physical, material or non-material damage to individuals such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy, or any other significant economic or social disadvantage to the individual concerned. Where personal data breaches do occur the Council will, without undue delay, seek to contain the harm to individuals, investigate the breach, report the breach to the Information Commissioner's Office and look to learn the lessons from any actual or suspected breaches.

2. Purpose

The aim of this policy and procedure is to ensure that the Council reacts appropriately to any actual or suspected personal data breaches in accordance with GDPR.

3. Scope

This document applies when a personal data breach is suspected. The policy and procedure it sets out is to be followed by all Councillors, officers, contractors and agents of the Council who use Council facilities and equipment, or have access to, or custody of, personal data collected by the Council.

4. Definitions

"Personal data" means any information relating to an identified or identifiable individual ('data subject'); an identifiable individual is someone who can be identified, either directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.

The definition of a "personal data breach" is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

A personal data breach includes, but is not restricted to, the following:

- The accidental alteration or deletion of personal data
- The transfer of personal data to those who are not entitled to receive it
- Unauthorised access to personal data
- Use of personal data for purposes for which it has not been collected and which go beyond those uses that the data subject could reasonably have contemplated
- Theft of storage devices

5. Risks

The Council recognises that there are risks associated with the collection, use transmission and storage of personal data in order to conduct official Council business. By following this policy and procedure, suspected data breaches should be identified quickly and the impact of personal data breaches should be reduced by ensuring suspected personal data breaches are followed up correctly and helping identify areas for improvement.

Non-compliance with this policy and procedure could result in significant detrimental effects on individuals and the Council being heavily fined and/or its reputation being damaged.

6. Procedure for reporting personal data breaches

Appendix 1 provides a high level process flow diagram illustrating the process to be followed when reporting suspected or actual personal data breaches.

Personal data breaches need to be reported to the Council's Data Protection Officer (Anna Goodall agoodall@fenland.gov.uk or 01354 62 2357) at the earliest possible stage as the Council has a duty to report any personal data breach to the Information Commissioner's Office (ICO) within 72 hours unless the ICO has issued guidance to the contrary.

The information provided to the Data Protection Officer should include as much detail as possible of the personal data breach, those affected and the consequences. A form is available on the Intranet to report a personal data breach – if not completed at the time of the actual report, it must be completed immediately afterwards. The Data Protection Officer and Member Services can assist in completing the form. The reporting of a suspected personal data breach should not be delayed however while the information is being gathered. The Data Protection Officer will make an assessment of whether the personal data breach passes the threshold (if any) set by the ICO for personal data breaches to be reported to the ICO. The Data Protection Officer will also make an assessment of the risk to the data subject. If the Data Protection Officer concludes that the personal data breach is likely to result in a high risk to the rights and freedoms of the data subject, for example, where there is a risk of identity theft, she will notify the data subject directly.

The Data Protection Officer will notify the Senior Information Risk Owner (SIRO), the Chief Executive and the Corporate Management Team (CMT) as soon as possible after receiving a report of a personal data breach. The SIRO, Chief Executive, Data Protection Officer, and CMT will agree what measures should be taken to deal with the personal data breach.

When reporting the breach to the ICO the Data Protection Officer will include the following information:

- The nature of the personal data breach including, where possible
- The categories and approximate number of individuals concerned
- The categories and approximate number of personal data records concerned

- The name and contact details of the Data Protection Officer or other contact point where more information can be obtained

- A description of the likely consequences of the personal data breach

- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

In the event that it is not possible to report the personal data breach to the ICO within 72 hours, the notification will also give the reasons for the failure to do so.

7. Policy Compliance

If any officer is found to have breached this policy and procedure, they may be subject to the Council's disciplinary procedure. If any councillor is likewise found to have breached the policy and procedure, a complaint will be made to the Conduct Committee. In either case if a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from the Data Protection Officer or SIRO.

8. Policy Governance

The following table identifies who within the Council is Accountable, Responsible, Informed or Consulted with regards to this policy and procedure. The following definitions apply:

- Responsible – the person(s) responsible for developing and implementing the policy.

- Accountable – the person who has ultimate accountability and authority for the policy.

- Consulted – the person(s) or groups to be consulted prior to final policy implementation or amendment.

- Informed – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	Data Protection Officer
Accountable	Chief Executive
Consulted	Senior Information Risk Owner, Management Team
Informed	All councillors, officers, contractors and agents.

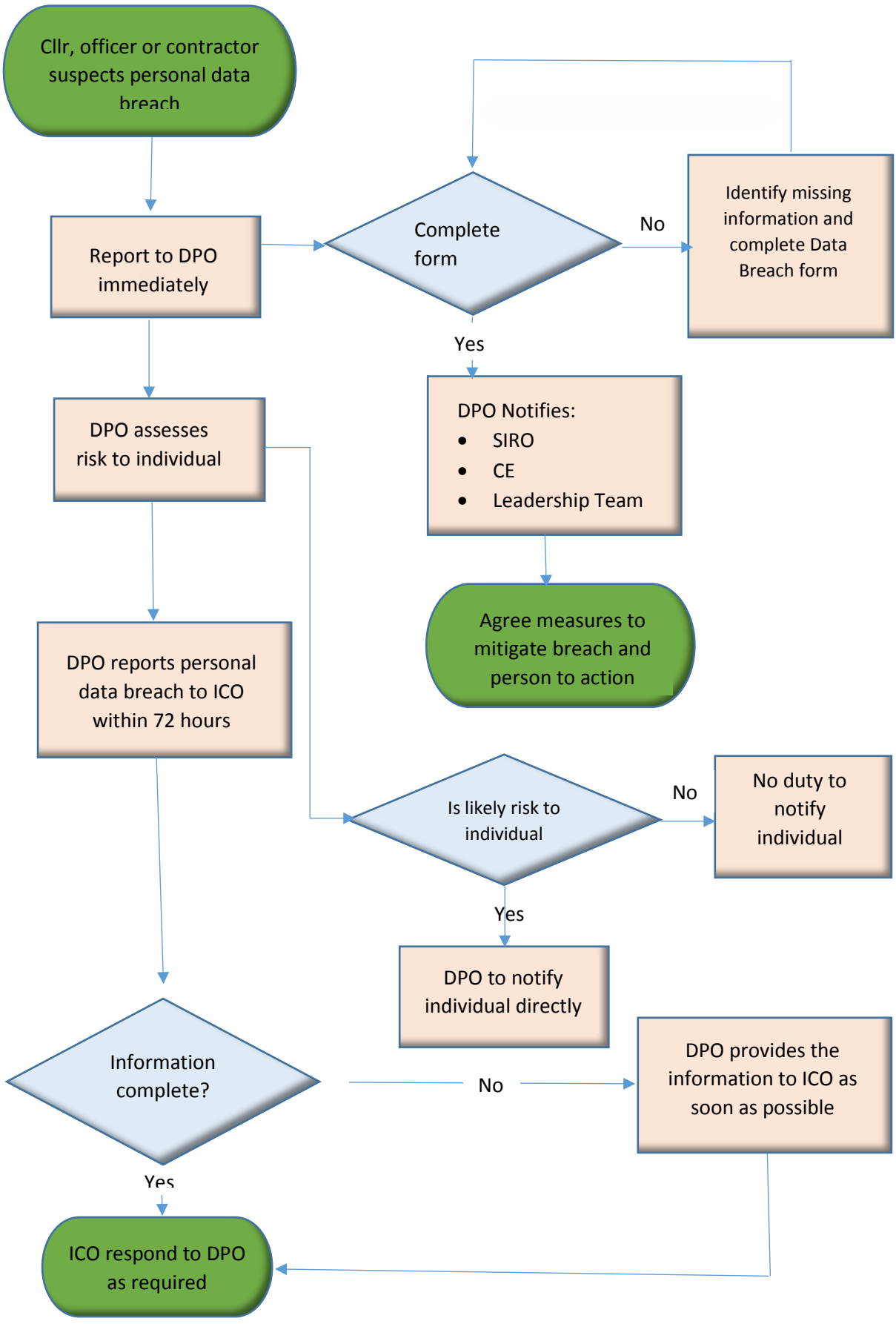
9. Review and Revision

This policy and procedure will be reviewed by the Data Protection Officer as it is deemed appropriate, but no less frequently than every 12 months.

10. Key Messages:

- A personal data breach is more than just losing personal data
- Personal data breaches can have significant impacts on individuals
- The Council has a duty to notify the ICO of any personal data breach and may have to inform individuals directly
- All councillors, officers, contractors and agents of the Council should report any suspected personal data breaches immediately
- There are potentially heavy fines for failing to report personal data breaches to the ICO.

Appendix 1 – Process Flow; Reporting a personal data breach



Appendix 2 - Breach Matrix – Including Impact Criteria

Breach Types
Lost in Transit - The loss of data (usually in paper format but may also include CDs, tapes, DVDs or portable media) whilst in transit from one service area to another. May include data that is: • Lost by a courier • Lost in the 'general post' (i.e. does not arrive at its intended destination) Lost whilst on site but in situ between two spate buildings or services (I.e. CHR & WSH)
Lost or stolen hardware - The loss of data contained on fixed or portable hardware. May include: • Lost or stolen Laptops • Hard drives • Pen drives • Servers • Cameras • Mobile phones – containing personal data • Desk-tops / other fixed electronic equipment • Imaging equipment containing personal data • Tablets The loss or theft could take place on or off a data controllers premises. For example the theft of a laptop from an employee's home or car, or a loss of a portable device whilst travelling on public transport. Unencrypted devices are at particular risk
Lost or stolen paperwork - The loss of data held in paper format would include any paper work lost or stolen which could be classified as personal data examples would include: • Housing assistance forms • Letters • Complaints • Registers • Officers notebooks The loss or theft could take place on or off a data controllers premises. For example the theft of paper work from an employee's home or car, or a loss of a portable device whilst travelling on public transport.
Disclosed in Error - This category covers information which has been disclosed to the incorrect party or where it has been sent or otherwise provided to an individual or organisation in error. This could include situations where the information hasn't actually been accessed. Examples include:

• Letters / assessments / files been sent to the wrong individuals • Verbal disclosures made in error • Failure to redact personal information from documentation to the requester or third parties – particularly in regards to DSARs • Inclusion of information relating to other data subjects in error – again particularly DSARs • Emails / faxes sent to the incorrect individual or with the incorrect information attached • Failure to blind carbon copy emails Mail merge / batching errors on mass mailing campaigns leading to the incorrect individuals receiving personal data
Uploaded to website in error - This category is distinct from disclosure in error as it relates to information added to a website containing personal data which is not suitable for disclosure. It may include: • Failures to carryout appropriate redaction • Uploading the incorrect documentation
Non-secure disposal of hardware - The failure to dispose of hardware containing personal data using appropriate technical and organisational means. It may include: • Failure to meet principle 6 of GDPR (Security) when employing a third party processor to carry out the removal / destruction of data • Failure to securely wipe data prior to destruction • Failure to securely destroy hardware to appropriate industry standards Re-sale of equipment with personal data still intact / retrievable
Non-secure disposal of paper work - The failure to dispose of paper work containing personal data using appropriate technical and organisational means. It may include: • Failure to meet principle 6 of GDPR (Security) when employing a third party processor to remove / destroy / recycle paper • Failure to use confidential waste destruction facilities Data sent to landfill / recycling intact
Technical security failure (including hacking) - The category concentrates on the technical measures a data controller should take to prevent unauthorised processing and loss of data and would include: • Failure to secure systems from inappropriate / malicious access • Failure to build website / access portals to appropriate technical standards • Failure to protect internal files sources from accidental / unwarranted access (for example failure to secure shared file spaces) In respect of successful hacking attempts, the ICO's interest is in whether there were adequate technical security controls in place to mitigate the risk

Corruption or inability to recover electronic data - Avoidable or foreseeable corruption of data or an issue which otherwise prevents access which has quantifiable consequences for the affected data subjects e.g. disruption care / adverse clinical outcomes, for example: • The corruption of a file which renders the data inaccessible The inability to recover a file as its method / format of storage is obsolete
Unauthorised access / disclosure - Wilful unauthorised access to, or disclosure of, personal data without the consent of the data controller
Other - This category is designed to capture the small number of occasions on which breach occurs which does not fall into the aforementioned categories. These may include: • The sale or recycling of office equipment (for example filing cabinets which later are found to contain personal data) Inadequate controls around physical employee access to data leading to the insecure storage of files (for example failure to implement a clear desk policy or insufficient lockable filing cabinets and storage)

Impact Criteria

Impact Levels	Harm Criteria	Damage to Council's reputation with the possibility of regulatory action and subsequent legal action from the data subjects against the council or council employees	Data Subject		
			Confidentiality	Integrity	Availability
1	*Negligible*	Minor harm to an individual, individuals or small group which could result in some publicity in the local media. No legal or regulatory consequences	Public information disclosed	Public information corrupted	Public information lost
2	*Low*	Harm to an individual, individuals or small group which could result in publicity in the local media and social media. Some legal or regulatory notification might be needed (i.e. advice from the ICO might be sought)	Semi Public or minor identifying information disclosed	Semi Public or minor identifying information corrupted	Semi Public or minor identifying information lost
3	*Moderate*	Minor damage or distress to an individual, individuals or a group, which could result in adverse publicity in traditional national media. Some legal or regulatory sanction (Notifiable)	Identifying information disclosed	Identifying information corrupted	Identifying information lost
4	*High*	Damage and distress to an individual or substantial number of individuals which could result in sustained adverse publicity in national and social media. Significant legal or regulatory sanction (Notifiable)	Identifying information disclosed	Identifying information corrupted	Identifying information lost
5	*Very High*	Significant damage and distress to an individual or high number of individuals which could result in sustained adverse publicity across all media platforms. Major legal or regulatory sanction (Notifiable)	Sensitive information disclosed	Sensitive information corrupted	Identifying information lost