Fenland
CAMBRIDGESHIRE
Fenland District Council

Data Protection Policy

February 2020

Contents

1. Introduction

1.1 The General Data Protection Regulation (GDPR) and Data Protection Act (DPA) were updated in 2018 to reflect technological advancements and changes since the last act in 1998. This policy outlines how Fenland District Council will adopt the provisions of the GDPR and DPA.

1.2 Higher fines have been introduced for data breaches and non-compliance. The Information Commissioner's Office (ICO) have the power to issue fines of up to 20 million Euros or 4% of a company's worldwide revenue dependent on which is the higher sum.

1.3 Major changes include stronger conditions for consent, the need for privacy controls to be built in at the design phase, greater rights for data subjects and tighter controls on data breaches.

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

2. Definitions

2.1 'Personal data' means any information relating to an identified or identifiable living individual ('Data Subject')

2.2 'Identifiable living individual' means a living individual who can be identified, directly or indirectly, in particular by reference to:

- An identifier such as a name, an identification number, location data or an online identifier

- One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual

2.3 '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

2.4 ‘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:

- Collection, recording, organisation, structuring, storage
- Adaptation or alteration
- Retrieval, consultation, use
- Disclosure by transmission, dissemination or otherwise making available
- Alignment or combination, or
- Restriction, erasure or destruction.

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

2.6 ‘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.

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

2.8 ‘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.

3. Policy Statement

3.1 Fenland District Council supports the objectives of GDPR and DPA and seeks to ensure compliance with this data protection legislation.

3.2 This policy aims 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, that it is held securely, that it is only held for as long as necessary and only shared with those who it needs to be shared with.

4. Scope

4.1 All staff and members, both permanent and temporary, are required to adhere to this policy. They have a responsibility for handling personal data safely, securely and in line with the council's policies. All volunteers, work placements and any agency workers are required to read and comply with this policy and GDPR requirements.

5. Aims and Objectives

5.1 This policy sets out the council's commitment to upholding the data protection principles outlined 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.

5.2 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.

5.3 In particular this policy aims to:

- Assist the council in complying 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.

5.4 The council also aims to mitigate the following risks through this policy:

- Accidental or deliberate breaches of the DPA and/or the GDPR
- Potential action against the council from the ICO due to the loss or misuse of personal data

- Potential legal action from any Data Subjects due to a breach of their data protection rights

- Potential reputational damage to the council as a result of any breaches of GDPR

5.5 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.

6. Roles and Responsibilities

6.1 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.

6.2 Members will be responsible for complying with this policy when engaging in council business and must be aware of their responsibilities as individuals. Whilst Fenland District Council acts as the controller and is therefore liable for violations regarding personal data, Councillors must be aware that it can be a criminal offence to process personal data outside of their role as a District Councillor or without due authorisation from the council. A serious breach of this policy by a member is a potential breach of the council's Members' Code of Conduct and would warrant investigation.

6.3 Overall responsibility for the GDPR and DPA will rest with the Senior Information Risk Officer (SIRO), Carol Pilson, in consultation with the Data Protection Officer, Anna Goodall. Anna can be contacted at AGoodall@fenland.gov.uk.

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

6.5 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. They must also monitor data protection compliance and increase awareness of both the DPA and GDPR across the council. The Data Protection Officer shall act as the contact point with the ICO.

6.6 The SIRO will take overall ownership of information security, act as champion for information risk at Corporate Management Team and provide written advice to the

Data Protection Officer on the content of the council's Annual Governance Statement in regard to information risk. The SIRO implements and leads the Information Governance (IG) risk assessment and management processes within the council and advises SLT on the effectiveness of information risk management.

6.7 The GDPR officer will be responsible for the practical implementation of data protection decisions, supporting the DPO, reviewing GDPR breaches and working in conjunction with the DPO to take forward any lessons learnt, advising and supporting staff and researching the approach by other authorities to inform FDC's approach.

6.8 Heads of Service will be responsible; for ensuring operational compliance with this policy within their own departments, for compiling and maintaining their Record of Processing Activities (ROPA) for his or her department and, for becoming involved in consultations with the Data Protection Officer when applicable.

6.9 All services are required to create and maintain their own privacy notices in consultation with the GDPR officer (Niall Jackson). The council shall inform individuals of its privacy information via its website, and will provide copies in such other reasonable format on request.

6.10 GDPR service champions are required to attend extra GDPR training on a yearly basis, attend regular meetings on data protection, disseminate what they have learnt across their service areas and make any necessary alterations within their service area to improve compliance with the GDPR and DPA.

6.11 All staff must understand the main concepts of GDPR, identify and report any risks to personal data security to the GDPR service champion and identify and report any data breaches to the DPO at the earliest possible time using the data breach reporting form which can be found on the intranet.

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

7. Council Statement on Data Protection Requirements

7.1 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's rights and freedoms are protected.

- The council will comply with Article 8 of the Human Rights Act 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 personal data held by the council will be kept in accordance with the six principles of the GDPR. The council will keep all electronic and manual records in accordance with its Data Retention Schedule.

- 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 Information management 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.

8. Data Protection Impact Assessment's

8.1 Data Protection Impact Assessment's (DPIA's) are a mandatory requirement under GDPR and are required when processing is likely to result in a high risk to individuals rights.

8.2 Before undertaking any new work stream or using any third party system/software which is likely to involve personal data, the council will carry out a DPIA.

8.3 DPIA's are a means of addressing a projects risk as part of overall project management. They are carried out with a view to identifying and managing any project risks relating to personal data which is collected, used, stored, distributed and destroyed throughout a project.

8.4 The function of the DPIA is to ensure that data protection risks are properly identified and addressed wherever possible, and that decision-makers have been fully informed of the risks and the options available for mitigating them. For those proposals that involve data sharing, this could include the risks if data is not shared.

8.5 The DPIA will set out information such as; the personal data to be collected, how it will be used, how it will be stored, whether it will be shared and for how long it will be retained.

8.6 Not every proposal will require a DPIA. The key questions in determining whether a DPIA is needed are:

- Will the proposal involve the processing of personal data of individuals?
- Is there a risk to the personal data or individuals' rights?
- Has a DPIA already been conducted for similar work?
- Do the ICO require you to do a DPIA?

8.7 DPIA templates have been provided for use on the council's intranet site.

9. Data Handling

9.1 Service areas must only collect the minimum amount of personal data that is necessary to fulfil their purposes. Service areas must not collect personal data on the basis that it may be useful, there must be a specific purpose.

9.2 When personal data is collected it must be ensured that the Data Subject is informed who the Data Controller is, the purpose(s) for which the personal data is to be used and any other information about how it will be used or shared. This can, and should, be provided in the form of a privacy notice.

9.3 The Information Security Policy should be adhered to in order to minimise the risk of a data breach.

9.4 Where applicable anonymisation or pseudonymisation techniques should be employed to protect personal data. These techniques should be utilised when necessary, particularly when sharing personal data with third parties.

9.5 All staff are responsible for ensuring that personal data is used and stored properly to prevent unauthorised access.

9.6 All personal data should:

- Be stored in locked desks or filing cabinets when not in use
- Only be accessed on secure council equipment and have limited access based on its sensitivity
- Not be visible on screens to unauthorised persons including the public and other members of staff
- Not be taken out of council offices or stored externally unless such use or storage is necessary and authorised by your line manager
- Only be kept for as long as is necessary and disposed of securely when no longer needed

9.7 All personal data held by service areas should be reviewed at regular intervals and deleted when it passes its retention date unless there are sufficient reasons to extend this period.

9.8 Duplicate records should be avoided to reduce the risk of inaccuracies and anomalies.

10. Contracts

10.1 Whenever the council uses a third party to process an individual's data on the council's behalf there must be a written contract in place.

10.2 The contract must include specific GDPR clauses surrounding the security of personal data and other data protection requirements such as access control, retention periods, and deletion of personal information. Sufficient procedures should be put in place regarding Subject Access Requests and complying with individuals' data rights such as the right to rectification.

10.3 The council shall ensure that they only use third parties who provide sufficient guarantees that the requirements of data protection law shall be met and the rights of individuals protected.

11. Information Requests

11.1 Requests from Data Subjects for copies of personal data that 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.

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

11.3 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.

11.4 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.

12. Prompt Replies to Requests

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

12.2 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.

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

12.4 In this instance the council will notify the applicant in writing that the Subject Access Request requires further time and will provide an estimate of a 'reasonable time' by which they expect a response to be made.

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

12.6 Unlike Freedom of Information requests, there is no upper cost or time limit for a Subject Access Request.

13. Exempting Information from Non-disclosure

13.1 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.

13.2 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

13.3 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.

14. Refusal of Subject Access Requests

14.1 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

14.2 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.

14.3 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.

14.4 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.

15. Data Breaches

15.1 This section should be read alongside the council's Reporting Personal Data Breaches policy.

15.2 A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

15.3 If any employee or member of the public becomes aware of a breach of the Policy, they should immediately report it to the Data Protection Officer who will be able to advise on any immediate action to be taken. The council have provided a Data Breach Reporting form on the intranet.

15.4 Upon receipt of notification of a breach, the Data Protection Officer will investigate the allegation and, if substantiated, identify an action plan which will include details of containment and recovery action, an assessment of the risks and identify any notifications that need to take place.

15.5 The GDPR requires all organisations to report certain types of personal data breaches to the ICO. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the council will also inform those individuals without undue delay.

15.6 Breaches must be reported to the ICO within 72 hours of the council becoming aware of the breach, where feasible.

15.7 The Data Protection Officer will consider the seriousness of the breach, the amount of data, the type of data, the number of customers affected, where the data is now located and whether it is recoverable or not.

15.8 If a Data Subject's personal data is disclosed outside of its intended purpose, they have a right to sue the responsible individual. Individual Officers and Members of the council may be prosecuted under GDPR, not just the council as a whole.

15.9 Deliberate breaches will result in disciplinary action under the Disciplinary (Conduct) policy based on each individual instance.

16. Appeals and Complaints

16.1 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

16.2 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

This Policy shall be held on both the council's intranet and public website

Appendix A

Data Protection Principles

Personal data must 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').

Appendix B

Conditions for Processing Personal Data

The basis for processing personal data must be lawful. At least one basis from the list below must apply whenever the council processes personal data:

a. Consent – the individual has given clear consent for the council to process their personal data for a specific purpose (Note: Consent can be withdrawn at any time)
b. Contract – the processing is necessary for a contract the council has with the individual, or because they have asked the council to take specific steps before entering into a contract.
c. Legal obligation- the processing is necessary for the council to comply with the law
d. Protect life – necessary to protect someone's life
e. Public task – the processing is necessary for the council to perform a task in the public interest or for the council's official functions, and the task or function has a clear basis in law
f. Legitimate interests – (but cannot be used for processing carried out by public authorities in the performance of their tasks)

Processing Special Category Personal Data

The glossary sets out the categories of special data which need to be processed with extra care. The special categories of personal data are subject to stricter conditions of processing. There are conditions for processing special categories of personal data, set out in Article 9 of GDPR and are summarised:

a. The Data Subject has given explicit consent, or
b. It is necessary for employment, social security or social protection law*
c. It is necessary to protect life or where an individual is physically or legally incapable of giving consent
d. It is carried out in the course of legitimate activities by certain not for profit organisations where it relates to specific persons
e. Where the personal data is manifestly made public by the individual
f. It is necessary for the establishment or defence of legal claims
g. It is necessary for reasons of substantial public interest*
h. It is necessary for purposes of preventative or occupational medicine and reasons relating to the provision of healthcare*
i. It is necessary in the interest of public health*
j. It is necessary for archiving purposes in the public interest or for scientific or historical research.*

Appendix C

Data Subject Rights

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)

Appendix D

1. Legal Framework and Relevant Legislation

- General Data Protection Regulation 2018
- Data Protection Act 2018
- The Criminal Justice and Immigration Act 2008
- The Environmental Information Regulations 2004 (SI 2004/3391)
- The Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426)
- The Regulation of Investigatory Powers Act 2000 (RIPA)
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699)
- Freedom of Information Act 2000
- Human Rights Act 1998
- Computer Misuse Act 1990
- This list is not exhaustive

2. Reference Documents

- Information Management Policy
- Information Security Policy
- Members' Code of Conduct
- Reporting Personal Data Breaches Policy and Procedures

Version Control

Policy name	Data Protection Policy			
Policy description	Alignment of policies and how to comply with Data Protection Act 2018 and General Data Protection Regulation			
Responsible Officer	Anna Goodall			
Version number	Date formally approved	Reason for update	Author	Review date
1.0	November 2019	Creation of Data Protection Policy	Anna Goodall	January 2020
2.0	February 2020	Altered structure to reflect FDC policy guidance. Added points on Contracts, DPIAs, Data handling and Data breaches	Anna Goodall	January 2021