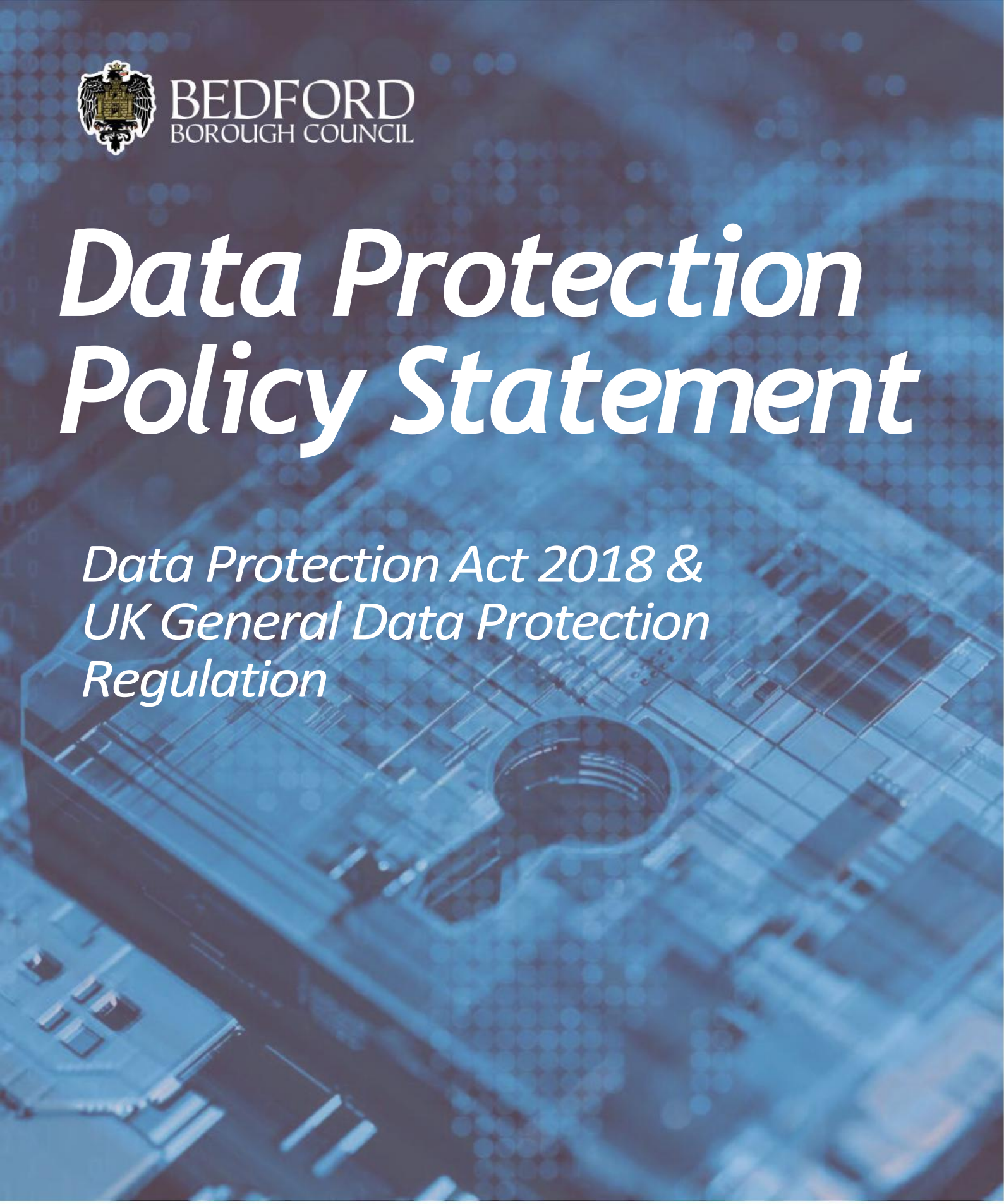
BEDFORD BOROUGH COUNCIL

Data Protection Policy Statement

Data Protection Act 2018 & UK General Data Protection Regulation



Data Protection Policy Statement

The Data Protection Act 2018 incorporates the requirements of the UK General Data Protection Regulation

BEDFORD BOROUGH COUNCIL

DATA PROTECTION ACT 2018 &

UK GENERAL DATA PROTECTION REGULATION

DATA PROTECTION POLICY

Index

Version History			
Date	**Version**	**Author**	**Brief Comments on Changes**
2001	1		Original Policy
17/12/2003	2	Michael Gough	Updated for Open Government commitments
2011	3	Keith Simmons	Update for responsibility changes
10/05/2018	4	Keith Simmons/	Updated for UK GDPR/DPA 2018
12/02/2019	5	Ann Jones	Update for responsibility changes
08/08/2024	6	Emma Pates	Updated to reflect changes in legislation and organisation structure

Introduction

Bedford Borough Council is a public authority governed by data protection legislation and is one of approximately 132 Councils in England that is a single-tier authority, meaning it is responsible for the complete range of principal Council functions and services within its area. These functions and services include[1]:

Arts and recreation	Libraries
Births, deaths and marriage registration	Licensing
Building regulations	Markets and fairs
Burials and cremations	Minerals and waste planning
Children's services	Museums and galleries
Civil Partnership registration	Parking
Community safety	Passenger transport (buses) and transport planning
Concessionary travel	Planning
Consumer protection	Public conveniences
Council tax and business rates	Public health
Economic development	Social services, including care for the elderly and community care
Education, including special Emergency planning educational needs, adult education, pre-school	Sports centres, parks, playing fields
Elections and electoral registration	Street cleaning
Emergency planning	Tourism
Environmental health	Trading standards
Highways (not trunk roads), street lighting and traffic management	Waste collection and recycling
Housing	Waste disposal

In delivering these services and functions, it is necessary to collect and use various types of information about individuals. Additionally, there is a need to process personal data of current, past, and prospective employees, suppliers, clients, customers, and other contacts. This also applies to Council Members in relation to their governance roles, the allowances payable to them, and to Independent and Co-opted Members.

In addition to the above, the Council is the Administering Authority for Bedfordshire Local Government Pension Scheme, and this role requires the processing of personal details of employees, former employees and their next of kin of admitted bodies within the scheme.

The Council is, in certain circumstances, appointed by another Data Controller to process personal data held by that Controller (e.g. in providing payroll, administrative and other support to that Controller).

In this statement the term 'processing' includes the collection, storage, deleting, searching, amending, and transferring of personal data unless it specifically sets out a more restricted definition.

Personal information must be dealt with properly however it is collected, recorded and used, whether on paper, in a computer, or recorded on other material and there are safeguards to ensure this in the Data Protection Act 2018 (DPA 2018) and UK General Data Protection Regulation[3] (UK GDPR).

The Council regards the lawful and correct treatment of personal information it holds as essential to successful operations, and to maintaining confidence between those with whom it deals with and itself. The Council ensures that it treats personal information lawfully and correctly.

To this end the Council fully endorses and adheres to the principles of data protection, as enumerated in the Data Protection Act 2018 and UK General Data Protection Regulation. Specifically, these principles require the Council to be responsible for compliance with this legislation in respect of personal data it is controller for and where it is the appointed processor for the data of another controller. The Council can demonstrate this by keeping records of compliance.

---

[1] Commons Library Research Briefing, 6 June 2024

[2] The Council is not the Data Controller for Electoral Registration and Elections (the Electoral Registration Officer is registered for this purpose with ICO notification number Z5916756), for the registration of Births, Deaths and Marriages (the Superintendent Registrar is registered with ICO notification number ZA172160), the casework role of Councillors (these are individually separately registered with individual notification numbers for the ICO).

[3] UK General Data Protection Regulation was introduced on 25 May 2

The Principles

a) to process **lawfully, fairly and in a transparent manner** in relation to individuals.

b) collect for specified, explicit and legitimate purposes and **not further process** 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 not be considered to be incompatible with the initial purposes.

c) it is adequate, relevant and **limited to what is necessary** in relation to the purposes for which it is processed.

d) it is **accurate** and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay.

e) is kept in a form which permits identification of data subjects for **no longer than is necessary** for the purposes for which the personal data is 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, subject to implementation of the appropriate technical and organisational measures required by the UK GDPR, in order to safeguard the rights and freedoms of individuals; and

f) 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.

The Council's Compliance with the Principles

The Council respects the rights of data subjects in relation to the personal data the Council processes. It will seek to do so in a transparent and open way to enable data subjects to exercise their rights. To this end, the Council has undertaken the following arrangements and commits to maintaining and refining these arrangements:

- An appointed Data Protection Officer (DPO) who shall have the role summarised on page 11 of this policy. At present the appointed officer is Jashpal Mann, Manager for Performance and Analytics.
- Seeks to raise awareness of the obligations of all staff and Members of the Council in relation to personal data the Council is the controller for. This includes mandatory Data Protection Essentials training available on the intranet via BBOLT.
- Specific training for those officers responsible for making decisions around how personal data is collected, held, accessed, shared and destroyed (otherwise called Information Asset Owners) to ensure that those decisions are taken with a knowledge of the requirements of the DPA 2018 and UK GDPR.
- A Corporate Record of Processing Activity (RoPA) setting out the detail around the legal basis of the processing of personal data across the Council, the purpose of the processing, where the personal data is received from and who it is disclosed to, the extent to which special category data is processed and the arrangements for storage of the data.
- Provides Privacy Statements at the points at which data subjects provide personal data or otherwise in advance or at the time that personal data is received from third parties. These notices consistently set out the Council's details as data controller, the purpose of the processing, the legal basis of the processing, the extent to which the personal data is shared with others, the retention/deletion details, how data subjects can exercise their rights and the compliance with equivalent safeguards for the processing of personal data.
- Providing a point of contact to exercise data subject rights separately from those of the service area.
- Reviewing and monitoring those areas where the Council utilise the consent of the data subject to ensure that this consent is informed, and clear arrangements are available to withdraw consent.
- Specific arrangements for recording and responding to data breaches; including circumstances when the Information Commissioner's Office (ICO) is informed of the breach and data subjects are informed.
- Pre-contractual due diligence checks of data processors seeking to be appointed by the Council, contractual conditions setting out the requirements of the Council for such processing of personal data, and the requirements for those processors to notify the Council of any / all data breaches and action consequential on the breaches.

- Written Data Sharing arrangements with those organisations the Council discloses personal data ensuring the rights of the data subject are preserved in that disclosure.
- Data Protection Impact Assessments are undertaken in respect of the processing of special category data (see definition in Appendix two) or where significant new systems / procedures are to be implemented for processing personal data.
- Physical security measures are in place at the official buildings it utilises for the processing of personal data; including as appropriate, physical barriers, restricted access systems and staff / security personnel to control access. In addition, CCTV is installed and operated as appropriate for purposes that include to act as both a deterrent and an evidence record for unauthorised access to personal data.
- Policies and procedures for staff working away from the official buildings referred to immediately above who take personal data out of those buildings to ensure safeguards are in place for that data.
- Cyber security tools (including firewalls) are deployed to prevent unauthorised access to personal data held on the Council's computer systems. In addition, classification systems require staff to identify email content as 'secure' where it contains personal data, this ensures the intended recipient can receive the intended material but in a way that keeps that data secure. Emails containing personal data should not be sent 'unsecure'.

Roles and responsibilities

The Information Governance Board is responsible for approving this policy for managing compliance with data protection legislation and the Corporate Leadership Team should be kept informed. 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 reviewing this document from time to time. All employees, workers, agency placements and contractors of the Council are responsible for ensuring that data subjects seeking to exercise their rights (including 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.

Information Asset Owners are responsible for ensuring operational compliance with data protection principles in respect of the information assets they have a responsibility for. Chief Officers and Directors have a responsibility to oversee these arrangements in the light of this policy within their own service areas/Directorates and for becoming involved in consultations with the Data Protection Officer when applicable.

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

General Conditions of Processing

In respect of the lawful conditions of processing personal data, the Council has identified for each processing activity which of the following lawful reasons it relies upon for that processing[4]:

- Consent to the processing of personal data for one or more specific purposes (Article 6(1)(a))
- Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract (Article 6(1)(b))
- Processing is necessary for compliance with a legal obligation (Article 6(1)(c))
- Processing is necessary to protect the vital interests of a data subject or another person (Article 6(1)(d))
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. (Article 6(1)(e))
- Processing is necessary for reasons of substantial public interest (Article 9(2)(g)) – (pertaining to special category data)

In many cases, the processing of personal data may be permitted for more than one of the above reasons.

[4] In a very limited set of circumstances, the Council may also be able to process personal data where the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. The view of the Data Protection Officer will be sought before this condition is to be relied upon.

Processing Conditions for Special Category Personal Data

The Council's obligations as a data controller are more exacting when it processes special category personal data. 'Special Category' personal data may be summarised as data that reveals a data subject's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used to uniquely identify natural persons, health data, data concerning an individuals' sex life, or sexual orientation.

At least one of the following conditions must also be satisfied in order to process sensitive personal data:

(a) **Explicit consent** of the data subject, unless reliance on consent is prohibited by law
(b) Processing is necessary for carrying out **obligations under employment**, social security or social protection law, or a collective agreement
(c) Processing is necessary to protect the **vital interests** of a data subject or another individual where the data subject is physically or legally incapable of giving consent
(d) Processing relates to personal data **manifestly made public** by the data subject
(e) Processing is necessary for the establishment, exercise or defence of **legal claims** or where courts are acting in their judicial capacity
(f) Processing is necessary for reasons of **substantial public interest on the basis of law** which is proportionate to the aim pursued and which contains appropriate safeguards
(g) Processing is necessary for the purposes of preventative or occupational medicine, for assessing the **working capacity of the employee**, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of law or a contract with a health professional
(h) Processing is necessary for reasons of public interest in the area of **public health**, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices
(i) Processing is necessary for **archiving purposes** in the public interest, or scientific and historical research purposes or statistical purposes.

Further guidance concerning procedures and practices, and the Council's obligations in relation to special category personal data, is available by way of the Council's intranet or (for those without access to the Intranet, from the DPO).

Personal Data of children

Where the Council processes data of children it will be mindful of its obligations to those data subjects and the requirement/expectation for the rights of data subjects to be exercised by parents or those exercising parental responsibility.

Data subject rights

Data subjects have the following rights:

- Right to access to their own data.
- 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).

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

- A Subject Access Request (SAR) is not made in writing
- The council is 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

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.
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 Councils' decision.

Subject Access Requests

A Subject Access Request can be accepted in writing, by email, fax or letter, or even via social networking sites, an online form is also available on the Council's website. Requests can also be accepted over the phone or face to face.

All Subject Access Requests should be logged with the Council's FOI / SAR Team.

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

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.

However, if the Council considers the request to be complex, they may extend the time by up to two extra calendar months. In this respect, a 'global' request for all personal data the Council holds on a data subject is likely to constitute a more complex enquiry and data subjects should be advised of this at the earliest opportunity. In this instance the Council will notify the applicant in writing that the request requires further time and will provide an estimate of a 'reasonable time' by which they expect a response to be made. This could be a full three months for a 'global' request.

Personal data processed only for research, statistical or historical purposes.

The Council makes provision for the retention of some personal data once the primary purpose of the collection of and processing of that data has concluded. Once identified and isolated for these purposes, the personal data may only be processed for research purposes in compliance with the relevant conditions as defined in the DPA 2018 and UK GDPR.

Data Protection Breaches

While all reasonable steps should be taken throughout the Council to prevent a data protection breach, where such a breach occurs, staff will act in accordance with the adopted "Data Breach Plan", see Appendix A below.

The Role, Tasks and Accessibility of the Data Protection Officer (DPO)

The DPO is not personally responsible for data protection compliance by the Council. As the data controller, responsibility remains with the Council to comply with the DPA 2018 and UK GDPR.

The role of the DPO

The DPO assists the Council to monitor internal compliance, inform and advise on the Council's data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority, i.e. the Information Commissioner's Office (ICO).

The DPO is independent, an expert in data protection, adequately resourced, and reports to the Corporate Leadership Team.

The Council will not penalise the DPO for performing its duties. The Council will ensure that any other tasks or duties it assigns to the DPO do not result in a conflict of interests with their role as a DPO.

The Council will ensure that the DPO has appropriate access to personal data and processing activities across the Council. In addition, the Council will ensure that the DPO has access to other services within the organisation so that they can receive essential support, input or information to undertake their role.

Tasks of the DPO

The DPO is tasked with monitoring compliance with the DPA 2018 and UK GDPR and other data protection laws, the Council's data protection policies, awareness raising, training, and audits.

The Council will take account of the DPO's advice and the information they provide on its data protection obligations.

When carrying out a Data Protection Impact Assessment, the Council will seek the advice of the DPO who also monitors the process.

The DPO acts as a contact point for the ICO. They co-operate with the ICO, including during prior consultations required on specific processing of personal data, and will consult on any other matter.

When performing their tasks, the DPO has due regard to the risk associated with processing operations, and considers the nature, scope, context and purposes of processing.

Accessibility of the DPO

The DPO is easily accessible as a point of contact for our employees, individuals and the ICO.

The Council has published the contact details of the DPO and communicated them to the ICO.

APPENDIX A

BEDFORD BOROUGH COUNCIL

Data Breach Plan

Version: V03

CONTENTS

Version Control

Version Number	Date	Review Date	Author	Reason for new version
02	April 2018	April 2020	Ann Jones	Policy to take account of changes made by the General Data Protection Regulation, Data Protection Bill 2018 and Article 29 guidance
03	August 2024	August 2026	Emma Pates	Updated to include new processes

1. Introduction

1.1. Bedford Borough Council has a duty under the UK General Data Protection Regulation (UK GDPR) to ensure that the personal data they process is kept safely and securely. This plan details how the Council will respond in the event of a personal data breach.

1.2 No matter how careful we are in trying to ensure that all the personal data which the Council process is kept securely and used with security in mind, the potential for a personal data breach will always remain. We need to have a system in place to enable us to deal with any such breach as quickly and as efficiently as possible.

1.3 The Council already has other procedures in place to ensure that we comply with the UK GDPR. See list below:

- Data Protection Policy
- Computer User Security Policy
- ICT Remote Working and associated ICT Policies: E-Mail Usage, Password Policy, Removable Media Policy and Mobile Device Policy
- Procedure for Removal of Files from the office
- CCTV Policy, Procedures and Guidelines

1.4 This Plan is provided for use by officers within the Council.

2. Purpose

2.1 This plan puts into place a procedure for dealing with any breaches of personal data which may occur, focusing on the steps to be taken once a breach has been discovered, and the processes staff should follow in compliance with UK GDPR.

2.2 Instances of the loss of personal data are rare in the Council; however, the potential impacts on individual service users of the loss of personal information and the consequences to the reputation of the organisation mean that we need to take swift and appropriate action in the event of a loss.

2.3 In addition, the Information Commissioner's Office (ICO) can impose significant fines on data controllers for serious contraventions of the UK GDPR.

2.4 The ICO also can serve an enforcement notice on a data controller if the ICO considers taking positive steps is also necessary to bring about compliance. It is possible to receive a fine and an enforcement notice.

2.5 This plan aims to provide a consistent approach and follows guidance provided by the ICO. However, dealing with incidents of breaches of data is complex; there

are many potential variables, and a balanced judgement needs to be taken on a case-by-case basis.

3. Aim

3.1 This plan sets out the Council's commitment to upholding the UK GDPR principles, and managing the information they hold fairly and lawfully. It seeks to ensure that any personal or special category (sensitive) personal information the Council has in its possession is kept safely and securely and that processes are in place to minimise or mitigate the impact of a personal data breach.

4. Roles and responsibilities

4.1 This plan will be reviewed every two years by the Corporate Leadership Team or earlier, if necessary.

4.2 Chief Officers will be responsible for ensuring operational compliance with this plan within their service areas and for seeking advice from the Data Protection Officer, when appropriate.

4.3 The Council's Data Protection Officer (DPO), is responsible for the provision of advice and guidance regarding this plan. The DPO can be contacted at dpo@bedford.gov.uk.

4.4 This plan sets out the roles and responsibilities of officers which are also set out at 8.5.

5. Ensuring breaches do not happen

5.1 The effects of personal data losses are not only felt by the individuals concerned, but also affect the efficiency of the service and the reputation of the Council as a whole.

5.2 It is important that all staff are aware of their responsibilities for handling personal information, keeping it secure and not disclosing it without proper cause. Chief Officers should ensure that all staff within their responsibility are familiar with the appropriate policies and procedures.

5.3 The Data Controller (the Council) has a responsibility to ensure appropriate and proportionate security of the personal data they hold. This is covered by the 6th principle of the UK GDPR which requires that all personal data is:

"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')"

5.4 To prevent the Council from being in breach of the requirements of the UK GDPR all Elected Members, officers (whether permanent or temporary) and all third parties acting on behalf of the Council (Data Processors) or joint data controllers must be aware of their corporate and personal responsibilities set out under the provisions of the UK GDPR.

5.5 Breaches may involve either criminal or civil liability, or both, depending on the circumstances, and may include both individual and corporate responsibility.

6. What is a personal data breach?

6.1 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 transmitted, stored or otherwise processed. This means that a breach is more than just losing personal data.

6.2 Such loss or release can occur in several ways:

- Loss or theft of equipment, which holds personal data e.g. laptops, tablets, CDs
- Loss or theft of hard copy documents
- Equipment failure
- Inappropriate access or unlawful access, allowing unauthorised use
- Human error
- Unforeseen incidents such as flood or fire
- Hacking attacks
- Information obtained by surreptitious or deceptive means (blagging)
- Information being released inappropriately

7. Types of personal data breaches

7.1 Breaches can be categorised according to the following three information security principles:

- 'Confidentiality breach' - where there is an authorised or accidental disclosure of, or access to, personal data.
- 'Availability breach' – where there is an accidental or unauthorised loss of access to, or destruction of, personal data.
- 'Integrity breach' – where there is an unauthorised or accidental alteration of personal data.

8. Dealing with a breach

8.1 As soon as a breach has been identified, the officer concerned must report the incident immediately to their Line Manager, or the next Senior Manager if their Line Manager is not available. It will depend on the circumstances whether the reporting will be in person, by email, or by telephone. It is paramount that the Line Manager, or Senior Officer is made aware of the breach without delay.

8.2 It is recommended that the Line Manager is at that point nominated as 'breach owner' and that the relevant Chief Officer is informed. The Council's Data Protection Officer must be informed immediately.

8.3 Elected Members who identify a breach relating to their role within the Council (not as a representative of their ward or a political party) should initially contact the Chief Officer of the department concerned.

8.4 It should be remembered that if a breach of personal data occurs where we are processing data on behalf of one of our partners, then the partner concerned must be notified immediately as they are the Data Controller. Similarly, should a breach of personal data originate from a partner organisation (acting as the Council's Data Processor), the effects of the breach on the Council should be assessed and the use of this policy should be considered to protect the interests of the Council, their customers and stakeholders.

8.5 If a breach is suspected to have occurred the following information will be required to assess the seriousness of the breach:

- The type of data involved
- How sensitive the data is
- If the data has been lost or stolen, whether there are any protections in place e.g. encryption
- What has happened to the data
- What could the data tell a third party about an individual
- The volume of data i.e. how many individuals' personal data are affected
- Who are the individuals whose data has been breached
- What harm can come to those individuals
- Are there wider consequences to consider e.g. loss of public confidence, negative publicity, financial implications

8.6 A breach should be reported as soon possible via the Council's reporting procedure; the form is located at the following link: Data Breach Notification form

8.7 If after the initial assessment a breach has been clearly identified then an incident response team shall be co-ordinated by the relevant Chief Officer. This should include the key officers involved in the breach and if appropriate, a representative from the Council's Legal Team nominated by the Senior Information Risk Owner (SIRO). If appropriate, it may also be worth alerting the Council's Manager for Communications & Marketing at this stage so they can be ready to deal with any media enquiries.

8.8 This plan also acknowledges the role of the Caldicott Guardian Representative, Simon White who can be contacted by email simon.white@bedford.gov.uk. Acting as the "conscience" of an organisation, particularly regarding social care, the Caldicott Guardian actively supports work to facilitate and enable information sharing, advising on options for lawful and ethical processing of information as required.

8.9 The relevant Chief Officer must also consider whether the police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

8.10 The key officers involved should be proportionate to the type of breach, for instance, a minor breach may require involvement of the following:

- Line Manager (breach owner)
- Data Protection Officer (DPO)
- Chief Officer

A serious breach, whether in terms of size of breach, or sensitivity of information, should involve the following:

- Senior Information Risk Owner (SIRO)
- Chief Officer
- Representative from the Legal Team
- Chief Officer for Personnel Services
- Line Manager (breach owner)
- Data Protection Officer (DPO)

8.11 Responsibility rests with the Chief Officer or their nominated deputy, in considering the action to be taken to:

- Protect the interests of the data subject/s
- Keeping the data subject/s informed (if appropriate, see 10.1 – 10.7)
- Ensure the continuing delivery of the service
- Protect the interests of the Council
- Liaise with the DPO on further action, to gain their view on potentially informing the Information Commissioner's Office (ICO)

8.12 Breaches will require not just an initial response to investigate and contain the situation but also a recovery plan including where necessary, damage limitation. Establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise. This could be isolating or closing a compromised section of the network, finding a lost piece of equipment, or simply changing access codes. Establish whether losses can be recovered, and damage can be limited.

8.12.1 If the breach involves documentation sent to the incorrect address, steps should be taken to retrieve the documents, this may mean an officer needs to the visit the address to collect the papers sent in error.

8.12.2 If an email has been sent in error, the recall function should be used without delay, if this is unsuccessful the incorrect recipient should be asked to delete and purge the email.

8.13 If the DPO feels the data subject needs to be made aware of the breach, or if the data subject brought the breach to the Council's attention initially, then it will be the responsibility of the Line Manager to notify the data subject of next steps and keep them informed throughout the investigation, providing them with the findings once the investigation is complete.

8.14 The risks in terms of the potential adverse consequences for individuals will need to be fully assessed. How serious or substantial are the consequences and how likely are they to happen?

8.15 The DPO / Business Partner for Information Governance will maintain a log of all personal data breaches that have occurred.

9. Notifying the Information Commissioner's Office (ICO)

9.1 The UK GDPR places a duty on all organisations to report certain types of data breaches to the Information Commissioner's Office (ICO).

9.2 In the case of a personal data breach the Council shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the ICO, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the ICO is not made within 72 hours, it shall be accompanied by reasons for the delay.

9.3 The UK GDPR states that a personal data breach should be reported to the ICO if the breach is likely to result in a risk to the rights and freedoms of the individuals concerned. By this it means discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage. It also requires that this is done on a case-by-case basis. If there is not a risk to rights and freedoms, the ICO does not need to be notified.

9.4 After carrying out a full assessment of the risk, the decision as to whether to inform the ICO would be made by the DPO.

9.5 If the decision is to notify the ICO, the DPO will act as liaison with the ICO. The DPO will also ensure that the Chief Executive and SIRO are informed of all reported breaches.

9.6 The Chief Officer and the DPO, in conjunction with the Chief Officer for Personnel Services will also need to consider whether any officer concerned with the breach will be subject to disciplinary procedures.

9.7 The notification referred to in paragraph 9.2 shall at least:

(a) Describe the nature of the personal data breach including, where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned
(b) Communicate the name and contact details of the DPO, or other contact point, where more information can be obtained
(c) Describe the likely consequences of the personal data breach
(d) Describe the measures taken or proposed to be taken by the Council to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects

9.8 Where, and insofar as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

9.9 The Council shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken, this documentation shall enable the ICO to verify compliance with the UK GDPR.

9.10 Failing to notify a breach when required to do so can result in a significant fine; this is at the discretion of the ICO.

10. Communication of a personal data breach to the data subject

10.1 When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Council shall communicate the breach to the data subject without delay. This risk exists when the breach may lead to physical, material or non-material damage for the individuals whose data has been breached. Examples of such damage are:

- Discrimination
- Identity theft or fraud
- Financial loss
- Damage to reputation

10.2 When the breach involves special category data that reveals racial or ethnic origin, political opinion, religion or philosophical beliefs, or trade union membership, or includes genetic data, data concerning health or data concerning sex life, or criminal convictions and offences or related security measures, such damage should be considered likely to occur.

10.3 The flow chart at appendix four illustrates the methodology in assessing the risk to the data subject. Further information regarding the methodology of assessing the risk to the data subject can be found in the Article 29 Guidelines on Personal data breach notification, under Regulation 2016/679 Section IV at the link below.

Article 29 Breach Report

10.4 The communication to the data subject shall describe in clear and plain language the nature of the breach and contain at least the information and the recommendations provided for in points (b), (c) and (d) of paragraph 9.7.

10.5 The communication to the data subject shall not be required if any of the following conditions are met:

a) The Council has implemented appropriate technical and organisational protection measures, and that those measures were applied to the personal data affected by the breach, particularly those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption.
b) The Council has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise.
c) It would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

10.6 The DPO will consult the ICO to seek advice about informing data subjects about a breach and on the appropriate messages to be sent to, and the most appropriate way to contact, individuals.

10.7 Consideration also needs to be given to any prospective equality issues that may arise from a breach e.g. the vulnerability of an individual affected by the breach.

11. Post breach evaluation

11.1 Once the immediate breach response actions have been completed it is important not only to investigate the causes of the breach, but to also evaluate the effectiveness of the response. Carrying on ‘business as usual’ may not be acceptable if systems, policies or allocation of responsibilities was found to be at fault. Improvements should be instigated as soon as possible and should be communicated to staff and recorded so the Council can be seen to have reacted in a responsible manner.

11.2 Those investigations into the cause of the loss of data should consider any staff capability or training issues that may be indicated and where appropriate, action may be considered under the Council's disciplinary procedure.

11.3 If the breach was caused, even in part, by systemic and ongoing problems, then action will need to be taken and procedures in place to prevent any recurrence in the future.

Appendix One - Examples of incidents

Examples of the most common information security incidents are listed below. Please note that this list is not exhaustive.

Malicious

- Secure folders being viewed when they should be restricted.
- Computer infected by a virus or similar.
- Finding data that has been changed by an unauthorised person.
- Unknown people asking for information which could gain them access to Council data e.g. a password or details of a third party.
- Accessing a computer database using someone else's authorisation e.g. someone else's user id and password.

Misuse

- Information passed to a third party without consent – verbally, in writing or electronically.
- Sending a sensitive email to 'All Bedford Borough Council staff', or unintended recipient.
- Receiving and forwarding chain letters, including virus warnings, scam warnings and other emails which encourage the recipient to forward to others.
- Use of unapproved or unlicensed software on the Council's equipment.
- Writing down your password and leaving it on display or somewhere easily found.
- Printing or copying confidential information and not storing it correctly or confidentially.
- Outlook (email) auto populating with incorrect addresses and not being checked.
- Outlook (email), incorrect use of cc function as opposed to bcc.
- Correspondence sent to incorrect email address / postal address / recipient – no checking or validation undertaken.
- Email addresses being recorded incorrectly.
- Redaction software not being used.
- Records not being kept up to date.
- Completed forms with information pertaining to other individuals sent instead of blank.
- Not checking correct attachments are sent with emails.
- Meeting invites sent to recipients who should not be included.
- Data made available on the Councils' website which should not have been in the public domain

Theft/Loss

- Theft/loss of a hard copy file
- Theft/loss of any of the Council's computer equipment.
- Documents unable to be located.
- Receiving unsolicited mail which requires you to enter personal data.

Appendix Two - Definitions

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.

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

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.

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

Data subject - means the identified or identifiable living individual to whom personal data relates.

Subject Access Requests (SAR) - is a request made by an individual to an organisation for access to the personal data that the organisation holds about them. Under data protection laws, organisations must provide a copy of the data, details about its processing, and information on data sharing within one month. SARs are generally free, but a fee may apply for excessive requests.

Data Protection Impact Assessment (DPIA) - is a process designed to identify risks arising out of the processing of personal data and to minimise these risks as far and as early as possible. DPIAs are important tools for negating risk, and for demonstrating compliance with the UK GDPR.

Appendix Three - Examples of personal data breaches and who to notify

Example	Notify the ICO	Notify the data subject	Notes
We stored a backup of an archive of personal data encrypted on a CD. The CD is stolen during a break-in.	No	No	If the data is encrypted, backups of the data exist, and the unique key is not compromised, this may not be a reportable breach. However, if it is later compromised, notification is required.
A power outage lasting several minutes at the Customer Contact Centre meaning customers are unable to call us and access their records	No	No	This is not a notifiable personal data breach, but still a recordable incident under Article 33(5) of the UK GDPR. This should be included in the Personal Data Breach Log.
We suffer a ransomware attack which results in all data being encrypted. No back-ups are available, and the data cannot be restored. On investigation, it becomes clear that the ransomware's only functionality was to encrypt the data and that there was no other malware present in the system.	Yes	Only the individuals affected are notified if there is a high risk and it is clear that others were not affected.	If, after further investigation, it is identified that more individuals are affected, an update to the ICO must be made and the additional step of notifying other individuals if there is a high risk to them.
Personal data of 5000 customers are mistakenly sent to the wrong mailing list with 1000+ recipients	Yes	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.	
A direct marketing email is sent to recipients in 'to' or 'cc' field, thereby enabling each recipient to see the email address of other recipients.	Yes, notifying the ICO may be obligatory if a large number of individuals are affected, if sensitive data is revealed (e.g. mailing list of a psychotherapist) or if other factors present high risks (e.g. the email contains the initial passwords).	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.	Notification may not be necessary if no sensitive data is revealed and if only a minor number of email addresses are revealed.
An individual phones to report having received a benefit letter intended for someone else. We undertake a short investigation (i.e. completed within 24 hours) and establish with reasonable confidence that a personal data breach has occurred, and it is a systemic flaw so that other individuals are or might be affected.	Yes	Only the individuals affected are notified if there is a high risk and it is clear that others were not affected.	If, after further investigation, it is identified that more individuals are affected, an update to the ICO must be made and the additional step of notifying other individuals if there is a high risk to them.

Appendix Four - Flow chart showing notification requirements