

# Data Protection Policy

Version number: 2.0  
November 2022

## Tracking


<b>Policy Title</b>	Data Protection Policy		
<b>SMT sign off</b>	(insert day) October 2022		
<b>Committee</b>	S&R	<b>Date approved</b>	November 2022
<b>Review due date</b>	24 months (Next review November 2024)	<b>Review completed</b>	
<b>Service</b>	Policy and Corporate Resources		
<b>Document Owner</b>	Data Protection Officer		

## Revision History

Revision Date	Revisor	Previous Version	Description of Revision
26 September 2022	Data Protection Officer	1	Updates to legislation and consequential amendments.

## Document Approvals

Each revision requires the following approvals:

Title	Name	Signature	Date
Head of Service	Andrew Bircher		23.11.22
Interim Chief Executive	Jackie King		
Strategy & Resources Committee	N/A		

---

## Contents

1. Objectives .....	4
<a href="#">2. Responsibilities.....</a>	<a href="#">5</a>
<a href="#">3. Data Protection Principles.....</a>	<a href="#">5</a>
4. Lawful Basis for Processing.....	7
5 Rights of an Individual .....	8
6. Data Security .....	10
<a href="#">7. Data Breach.....</a>	<a href="#">11</a>
8 Information Sharing.....	14
9. Accountability and Governance .....	14
<a href="#">10. Training.....</a>	<a href="#">14</a>
Appendix 1: Definitions.....	16
Appendix 2: Data Protection Breach Notice Procedure.....	18
Appendix 3: Data Protection Breach Notification Form .....	19
Appendix 4: Data Breach Procedure Flowchart .....	22

## 1. Objectives

- 1.1. This Policy sets out how the Epsom & Ewell Borough Council (the council) complies with its duties under the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA) (together referred to in this document as 'the legislation').
- 1.2. All employees (including temporary employees) and Members are expected to comply fully with this policy and the principles laid down in the legislation (set out in Section 3 below). Members should adhere to the policy so as to ensure compliance with the Members' Code of Conduct and the council's obligations in relation to confidentiality.
- 1.3. The council supports the objectives of the legislation. This policy is intended to maintain the confidentiality of personal data held or processed either on computer or in manual files by the council and its contractors and to increase the access given to individuals to information relating to them.
- 1.4. This policy also covers what to do in the event of a Data Breach. An employee should contact their manager immediately and notify the Data Protection Officer (DPO). A Member should notify the DPO. The DPO is responsible for determining whether a breach has occurred and needs to be reported and must be made aware of all the facts immediately. Please see Appendix 2 for the Data Protection Breach Notification Procedure.
- 1.5. The legislation controls how personal information is used by organisations, businesses or the government. The Data Protection Act 2018 is the UK's implementation of the GDPR.
- 1.6. The law covers both written and computerised information and regulates any processing operation, including collection, storage, use, disclosure and destruction. The legislation ensures an individual's right to see such records. It is important to note that the legislation also covers records relating to employees and volunteers.
- 1.7. The council needs to process personal data and sometimes sensitive personal data about people with whom it deals in order to carry out its statutory duties, perform its functions and to comply with terms of contracts it has entered. This includes information on current, past and prospective service users, employees, suppliers, clients, customers, and others with whom it communicates. It may include all persons who live, work or visit the borough and many others who do not.
- 1.8. The council regards the lawful and correct treatment of personal information as critical to the success and effectiveness of its operations, and to maintaining the confidence of those it serves. It is essential that it respects the rights of all persons whose personal information it holds, that it treats personal information lawfully and correctly in accordance with the legislation and that it is able to show that this is the case.

- 1.9. Failure to comply with the legislation infringes the rights of individuals and may place them at risk of loss or harm. It also exposes the council to challenge legal claims and substantial financial penalty.
- 1.10. Guidance on data protection legislation published by the UK Information Commissioner's Office (the ICO) can be accessed on the ICO website.

## 2. Responsibilities

- 2.1 The Chief Executive has overall responsibility for ensuring the council's compliance with this Policy and with legislation.
- 2.2 The Data Protection Officer (DPO) has day-to-day responsibility for monitoring compliance with this Policy, advising the organisation on data protection matters and for receiving reports of personal data incidents for escalation as appropriate.
- 2.3 The Head of IT is the Senior Information Risk Officer with oversight of data protection and other aspects of information governance.
- 2.4 The Strategic Management Team (SMT), and Heads of Service (CMT) are responsible for:
  - ensuring that all systems, processes, records and datasets within their business area are compliant with this Policy and with data protection legislation;
  - assisting the DPO in their duties through providing all appropriate information and support;
  - ensuring that their staff are aware of their data protection responsibilities;
  - consulting the DPO on new developments or issues affecting the use of personal data in the organisation;
  - ensuring that Data Protection Impact Assessments are conducted as appropriate on data processing activities in their business area and drawing on advice from the DPO.
- 2.5 IT is responsible for procurement, technical security and issue of council IT equipment and assets. This includes the general provision and stability of the council's IT infrastructure and disaster recovery processes. IT is also responsible for the maintenance of records held about equipment, assets and their owners. They must also investigate, manage and resolve the IT aspects of data security breaches.
- 2.6 All employees of the council are responsible for understanding and complying with relevant policies and procedures for handling personal data appropriate to their role and ensuring that personal data processed by the council is accurate, up-to-date and secure. Any incident or breach affecting personal data held by the Council must be reported immediately in accordance with established procedures.

### 3. Data Protection Principles

As a data controller, the council is required to comply with the principles of Data Protection legislation. The legislation places a responsibility on every data controller to process any personal data in accordance with the data protection principles set out below.

#### 3.1. These principles require the Data Controller to:

- 3.1.1. Process personal data fairly, lawfully and in a transparent manner;
- 3.1.2. Obtain personal data only for one or more **specified** and **lawful purposes** and to ensure that such data is not processed in a manner that is incompatible with the purpose or purposes for which it was obtained;
- 3.1.3. Ensure that personal data is **adequate, relevant and limited to** the purpose or purposes for which it is held;
- 3.1.4. Ensure that personal data is **accurate** and, where necessary, **kept up-to-date**;
- 3.1.5. Ensure that personal data is not kept for any longer than is necessary for the purpose for which it was obtained;
- 3.1.6. Ensure that data is processed in a manner that ensures appropriate security of the personal data, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.

#### 3.2. Therefore, in practice the council must ensure that:

- 3.2.1. Personal data should only be processed when an appropriate lawful basis in the legislation can be identified;
- 3.2.2. Personal data should only be accessed by those who need to for work purposes;
- 3.2.3. Personal data should not be divulged or discussed except when performing normal work duties (see Paragraph 8 below for provisions on Data Sharing);
- 3.2.4. Personal data must be kept safe and secure at all times, including at the office, in public areas, at home or in transit;
- 3.2.5. Personal data should be regularly reviewed and updated; and
- 3.2.6. Queries about data protection, internal and external to the council must be dealt with effectively and promptly.

## 4. Lawful Basis for Processing

- 4.1. When processing personal data, there must be a valid reason for processing it, known as 'a lawful basis for processing'.
- 4.2. The lawful bases for processing are defined in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

Consent:	the individual has given clear consent for you to process their personal data for a specific purpose.
Contract:	the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
Legal obligation:	the processing is necessary for you to comply with the law (not including contractual obligations).
Vital interests:	the processing is necessary to protect someone's life.
Public task:	the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
Legitimate interests:	the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply to a public authority processing data to perform official tasks.)

### Sensitive Personal Data

- 4.3 Sensitive personal data, also known as special category data, is that which relates to a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life data, sexual orientation data, gender reassignment data, criminal convictions or offences or health data. If the information we are processing is 'sensitive personal data', we need to identify both a lawful basis for processing and a special category condition for processing in compliance with Article 9 of the GDPR.
- 4.4 To process sensitive personal data, you need one of the conditions above and one of the following grounds:
- Explicit consent for specified purpose;
  - Legal obligations of the council;
  - Vital interests of the individual or another where the individual cannot consent;
  - Manifestly made public by the data subject;
  - Exercise or defence of legal claim.
- 4.5 When processing sensitive personal data, you must document both the lawful basis for

processing and your special category condition so that you can demonstrate compliance and accountability.

## 5 Rights of an Individual

- 5.1 Under the legislation an individual has the following rights with regard to those who are processing their data:

### **The right to be informed**

- 5.2 The right to be informed covers some of the key transparency requirements of GDPR. It is about providing people with clear and concise information about what you do with their personal data. This is achieved by:
- Transparent information and communication;
  - Publishing fair processing notices that apply when collecting data from an individual or from third party.

### **The right of access**

- 5.3 This is the right of the individual to request a copy of their personal data (formally known as a subject access request).

### **The right to rectification**

- 5.4 The right to have information amended if it is incorrect or out of date.

### **The right to erasure (or right to be forgotten)**

- 5.5 Individuals have a right to have their data erased and to prevent processing in specific circumstances:
- Where data is no longer necessary in relation to the purpose for which it was originally collected;
  - When an individual withdraws consent (where the information is processed on the basis of consent);
  - When an individual objects to the processing and there is no overriding legitimate interest for continuing the processing;
  - Personal data was unlawfully processed.
- 5.6 If processing is necessary in some way, the individual may not have the right to erasure but may be able to restrict processing (see below).

### **The right to restrict processing**

- 5.7 An individual has a right to restrict processing. Where processing is restricted, the council is permitted to store the personal data but not further process it and will only be able to process it for the legal obligation or public task for which we require the information. (An individual cannot restrict processing or request erasure where the council is required to perform a public function, i.e. collecting council tax).

## **The right to data portability**

- 5.8 This relates to a person's right to have a data set from the data controller. However, it only relates to certain data. The data must be automated and held electronically. The information must also have been provided either by consent or as a means of processing a contract. Therefore, information collected by the Council for the purpose of a public task will be excluded. The DPO will be consulted in the event of any uncertainty in this regard.

## **The right to object**

- 5.9 Individuals have the right to object to the processing of their personal data. The right to object only applies in certain circumstances. Whether it applies depends on your purposes for processing and your lawful basis for processing. The DPO will be consulted in the event of any uncertainty.

### **When does the right to object apply?**

- 5.10 Individuals have the absolute right to object to the processing of their personal data if it is for direct marketing purposes.
- 5.11. Individuals can also object if the processing is for:
- a task carried out in the public interest;
  - the exercise of official authority vested in you; or
  - your legitimate interests (or those of a third party).
- 5.12 An individual must give specific reasons why they are objecting to the processing of their data. These reasons should be based upon their particular situation.
- 5.13 In these circumstances this is not an absolute right, and you can continue processing if:
- you can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
  - the processing is for the establishment, exercise or defence of legal claims.

## **Rights in relation to automated decision- making and profiling**

- 5.14 Automated decision-making is a decision made by automated means without any human involvement. The GDPR restricts decisions based solely automated methods, including those based on profiling, that have a legal or similarly significant effect on individuals.

Profiling relates to any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a person, in particular to analyze or predict aspects concerning that person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

- 5.15. In relation to automated decision-making and profiling, an individual has the right to request a human to review the decision.

## Processing requests from data subjects

- 5.16 The Data Protection Officer will ensure appropriate processes are in place to ensure the council enables the exercise of these rights, according to the provisions of the legislation.
- 5.17 Any information rights requests are processed by the Data Protection Officer and their team. Individuals will be expected to submit requests in writing and provide any necessary proof of identification as part of the request.
- 5.18 The council aims to respond promptly to these information rights requests and, in any event, within the statutory time limit of one calendar month. The deadline may be extended by a further two months if the request is complex or if we have received a large number of requests from the same person. Requests will be managed and tracked by Business Support.

## 6. Data Security

- 6.1 The council processes personal data and must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data.
- 6.2 The sixth principle of the Data Protection Act 2018 protects the integrity, privacy and confidentiality of data by placing specific obligations on organisations to secure it. To ensure compliance with this provision, all council employees must adhere to the following policies: Data Protection Policy, Information Assurance Policy, ICT Assurance and Acceptable Use Policy, Freedom of Information Policy, Environmental Information Policy and the Data Retention Policy.
- 6.3 These policies help safeguard our information security and ensure employees act in a manner that protects personal data. It is important we ensure we do everything possible to minimise the risk of a data breach occurring.
- 6.4 All employees are responsible for ensuring that personal data which they use or process is kept securely and is not disclosed to any unauthorised person or organisation. Access to personal data should only be given to those who have and can show a need for access to the data for the purpose of their duties.
- 6.5 Personal data should not be left where it can be accessed by persons not authorised to see it or have access to it by reference to this policy and the principles in the legislation.
- 6.6 Personal data which is no longer required must be destroyed appropriately, for example, by shredding or, in the case of computer records, secure deletion. When required, computers must have all personal information securely deleted using the appropriate software tools. Personal data must be destroyed in accordance with the council's Data Retention Policy.
- 6.7 Employees and Members who work from home must have particular regard to the need to ensure compliance with this Policy. The security and proper processing of data outside offices and usual places of work and whilst travelling must be ensured.

- 6.8 The DPO is responsible for determining whether a breach has occurred and must be made aware of all the facts immediately. Please see Appendix 3 for the reporting form.

## 7 Data Breach

### What is a data breach?

- 7.1. A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.
- 7.2. The table below sets out types of breaches with examples:

Breach Type	Definition	Example
Information disclosed in error	Where personal data is disclosed to an unauthorised party due to human or technical error	Email forwarded on to incorrect email address; fax sent to wrong number; paperwork posted to wrong person
Lost information or lost hardware	Where personal data or hardware containing personal data has been lost or misplaced	Lost memory stick, camera, lost paper file
Information lost in transit	Where personal data has been lost or gone missing after being sent from A to B by post or email	Royal Mail post lost in transit; email not received
Non-secure disposal of information or hardware	Where personal data is not disposed of securely	Confidential paperwork was not shredded; redundant laptop has not been decommissioned/wiped; memory stick not cleared
Stolen information or hardware	Where personal data or hardware containing personal data has been stolen	Theft of IT equipment, paper files stolen due to insecure filing
Technical or procedural failure	Where personal data is not necessarily disclosed but we are advised of a breakdown in security arrangements which placed data at risk of disclosure	Virus detected, website/email encryption failure, terminal left logged in and unattended in public area
Other	When you are unsure what definition	If none of the Breach Types are suitable

- 7.3 If the breach has occurred externally with one of our contractors or external systems providers, they have an obligation to notify us immediately and we must follow this procedure upon becoming aware of the breach.

## Who do we report a breach to?

- 7.4. In the event of a potential data breach, the relevant employee and manager, or Member, must alert the Data Protection Officer (DPO). The DPO is responsible for determining whether a breach has occurred and must be made aware of all the facts immediately. If the DPO determines a data breach has occurred, the DPO shall ensure that personal data breaches are investigated and, where the breach is likely to pose a risk to the rights and freedoms of individuals, report the breach to the Information Commissioner's Office (the ICO) in line the requirements of the legislation. Appendix 2 sets out the reporting process for a data breach.

## How much time do we have to report a breach?

- 7.5 The DPO must report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it. If it takes longer than this, reasons for the delay are required to be given. The DPO needs to report to the ICO within this time period whether or not we have collected all the relevant information. Supplemental information can be provided after the initial reporting (but again this needs to be done with reasonable haste and proper prioritisation given to the reporting).
- 7.6 If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the council must also inform those individuals without undue delay.

## What to do when a data breach occurs?

If it is suspected that a data breach has occurred (or may have occurred), it is important to escalate the incident immediately by completing the following steps. The DPO is responsible for determining whether a breach has occurred and must be made aware of all the facts immediately.

**Table: Steps to take if a data breach occurs**

Step	Action
1	Inform your Manager and the Data Protection Officer (DPO) immediately.
2	Manager needs to immediately inform ICT.
3	Fill out the Data Protection Breach Notice form (Appendix 3).
4	Send the form to the DPO (dataprotectionofficer@epsom-ewell.gov.uk) and your Manager as a matter of urgency.
5	After you have reported the incident to the DPO using the reporting form, you will need to liaise with the DPO regarding next steps.
6	In consultation with your manager and the DPO, you may need to contact the individuals whose personal data has been mishandled.
7	The DPO will then assess the Data Protection Breach Notice form. The DPO will determine whether the ICO needs to be informed of the breach.

## **What information must a breach notification contain?**

7.7 When reporting a breach, you must provide:

- a description of the nature of the personal data breach including, where possible;
  - the categories and approximate number of individuals concerned and
  - the categories and approximate number of personal data records concerned.
- the name and contact details of the DPO or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

7.8 The Data Protection Breach Notice form sets out the information needed to report a breach.

## **Confidentiality Issues**

7.9 If you feel you cannot tell your manager or other staff members via this reporting procedure, you should report the incident via the council's Whistleblowing Policy.

## **What breaches do we need to notify the ICO about?**

- 7.10 When a personal data breach has occurred the DPO will establish the likelihood and severity of the resulting risk to peoples' rights and freedoms. If it's likely that there will be a risk, then the DPO will report to the ICO if necessary. If it is unlikely that there are any risks to peoples' rights and freedoms, then it will not need to be reported. The breach will, however, still need to be documented.
- 7.11 In assessing risk to rights and freedoms, it's important to focus on the potential negative consequences for individuals.
- 7.12 A breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. The breach will be assessed on a case-by-case basis, looking at all relevant factors.

## **When do we need to tell individuals about a breach?**

- 7.13 If a breach is likely to result in a high risk to the rights and freedoms of individuals, the procedure set out in Appendix 2 to this Policy must be followed.
- 7.14 The DPO will need to make an assessment, based on the facts of the breach, to determine the level of risk to the rights and freedoms of the individuals involved. In making that determination, the DPO will assess both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring.

## 8 Information Sharing

- 8.1 Personal data may need to be shared with third parties in order to deliver services or perform our duties. The council will only share personal data when a lawful basis from the legislation can justify that sharing, where it is necessary to achieve a clear purpose and, with that purpose in mind, it is fair and proportionate to do so.
- 8.2 Disclosure within the council either to staff or elected Members will be on a need-to-know basis or to enable the most effective discharge of their responsibilities. Such disclosure may only be carried out when a lawful basis from the legislation can justify that disclosure. It will be carried out in accordance with the principles laid down in the legislation.
- 8.3 Data Sharing Agreements should be put in place when setting up on-going or routine information sharing arrangements with third parties. All Data Sharing Agreements must be signed off by the Data Protection Officer, who will keep a register of all Data Sharing Agreements.<sup>1</sup>
- 8.4 The council must ensure that personal data is not transferred to a country outside the European Economic Area unless the country to which it is sent ensures an adequate level of protection for the rights (in relation to the information) of the individuals to whom the personal data relates.

## 9. Accountability and Governance

### Contracts

- 9.1 Third parties such as partners, public and private organisations or contractors with whom the council shares personal data or who hold data on the council's behalf will be expected to enter into and adhere to formal agreements or contractual obligations with the council incorporating the principles of this policy and the requirements of the legislation. Such agreements or contracts must define the purposes for which personal data is supplied to or held by the other party and require contractors to have in place appropriate organisational and technical measures to protect the data and processes to enable the exercise of the rights of individuals.

### Documentation

- 9.2 The legislation sets out documentation obligations for every organisation. The council is required to keep records demonstrating compliance with the legislation. The council must keep records on the following:
  - The lawful basis for processing (as set out in paragraph 4 above);
  - Data sharing arrangements;
  - Retention Schedule;
  - Description of technical and organisation security measures.
- 9.3 The council is maintaining these records within its Asset Registers. Every Service Area has an Asset Register detailing the required information as set out above. Each Head of

---

<sup>1</sup> The review and maintenance of the Data Sharing Agreements Register is ongoing as at October 2022.

Service will review their Asset Registers on an annual basis and send a copy to the Business Assurance Manager and the Data Protection Officer.

## **Data Protection Impact Assessments**

9.4 As required by legislation, Data Protection Impact Assessments ('DPIAs') will be completed in instances when the processing of personal data is likely to result in a high risk to the rights and freedoms of individuals. The DPIA will be completed by the Manager and signed off by the DPO.

9.5 Such instances may include, but are not limited to:

- Introduction of new technologies or any significant changes to how we process/share data;
- Systematic and extensive processing activities;
- Use profiling or automated decision-making to help make decisions on someone's access to a service, opportunity or benefit;
- Large scale processing of sensitive or special categories of data or personal data relating to criminal convictions or offences;
- Large scale, systematic monitoring of public areas, such as CCTV; and
- Before entering a data sharing agreement.

## **10 Training**

10.1 Data protection training is important so that all employees and elected Members understand their responsibilities.

10.2 Mandatory e-Learning training as part of the induction process, and annual refresher training is undertaken by all employees and is made available to Members. The Data Protection Officer shall ensure that training resources are up to date, and that they are promoted within the council to ensure the take up of training and advice by employees.

## Appendix 1: Definitions

Term	Meaning
Data Controller	<p>The entity with overall responsibility for data collection and management. The data controller is responsible for determining the purpose and manner in which personal data is processed. Data controllers are required to be registered with the ICO.</p> <ul style="list-style-type: none"> <li>• Epsom and Ewell Borough Council (and its employees) is a Data Controller for the purpose of the Act and is registered as such.</li> <li>• The EEBC Councillors are all separately registered in their own right as Data Controllers.</li> <li>• The Electoral Registration Officer and Returning Officer are also Data Controllers and are also separately registered as such.</li> <li>• The Epsom &amp; Ewell Property Investment Company Limited is a Data Controller and is separately registered as such.</li> </ul>
Data Processor	An individual (other than an employee of the council) or organisation handling or processing data on behalf of the council.
Data Protection Officer	<p>The Data Protection Officer.</p> <p>The DPO is responsible for monitoring internal compliance, advising on data protection obligations and compliance, reviewing Data Protection Impact Assessments (DPIAs) and acts as a contact point for data subjects and the supervisory authority (Information Commissioner's Office).</p>
Data Subject	A living individual about whom data is held.
Personal data	Any information which enables a person to be identified either through their name or another identifier such as an identification number.

Processing of information	Refers to how information is held and managed. Processing can be any operation performed on personal data, whether or not by electronic or automated means, such as collection, use, storage, disclosure or destruction.
Profiling	Relates to any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
Sensitive personal data/ also known as special categories of personal data	<p>Special category data is more sensitive, and so needs more protection. Therefore to process this data, there are extra conditions for processing.</p> <p>Special categories personal data includes information relating to:</p> <ul style="list-style-type: none"> <li>• racial or ethnic origin of the data subject;</li> <li>• their political opinion;</li> <li>• their religious beliefs or other beliefs of a similar nature;</li> <li>• whether they are a member of a trade union;</li> <li>• their physical or mental health or condition;</li> <li>• genetics;</li> <li>• biometrics (where used for ID purposes);</li> <li>• their sexual life;</li> <li>• sexual orientation;</li> <li>• gender reassignment;</li> <li>• criminal offences or convictions.</li> </ul>

**What must you do first?**

1. Inform your Manager and the Data Protection Officer (DPO) immediately. Members are to inform the DPO immediately.
2. Manager needs to immediately inform ICT.
3. Fill out the [Data Protection Breach Notice Form \(see Appendix 3 of this policy\)](#).
4. Send the form to the DPO and your manager as a matter of urgency.
5. After you have reported the incident to the DPO using the reporting form, you will need to liaise with the DPO regarding next steps.
6. In consultation with your manager and the DPO, you may need to contact the individuals whose personal data has been mishandled.
7. The DPO will then assess the Data Protection Breach Notice Form. The DPO will determine whether the ICO needs to be informed of the breach.

**What information must a breach notification contain?**

When reporting a breach, the legislation says you must provide:

1. a description of the nature of the personal data breach including, where possible;
2. the categories and approximate number of individuals concerned; and
3. the categories and approximate number of personal data records concerned;
4. the name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
5. a description of the likely consequences of the personal data breach; and
6. a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

Most of this information is included in [the Data Protection Breach Notice Form](#).

### Data Protection Breach Notification Form

Reporting department	
Officer reporting breach	
Date of breach	
Nature of potential data security breach  (please include category of personal data involved <sup>2</sup> , how many individuals have been involved and the type of individuals involved <sup>3</sup> )	
What happened?	
Please describe the possible impact on the data subjects as a result of the breach. Please state if there has been any actual harm to the data subjects and also assess the likelihood of whether they will experience significant consequences (e.g. to their rights as data subjects, see Data Protection Policy).	
What has been done to contain the breach and/or recover the data?	
What are the risks?	

---

<sup>2</sup> Data revealing sensitive personal data = racial or ethnic origin, Political opinions, Religious or philosophical beliefs, Trade union membership, Sex life data, Sexual orientation data, Gender reassignment data, Criminal convictions or offences, Health data. Basic personal identifiers = eg name, address, contact details, Identification data eg usernames, passwords, Economic and financial data eg credit card numbers, bank details, Official documents eg driving licences, Location data, Genetic or biometric data, Not yet known, Other (please give details).

<sup>3</sup> Employees, Users, Subscribers, Students, Customers or prospective customers, Patients, Children, Vulnerable adults, Deceased individual, Not yet known, Other (please give details)

<p>Does the Information Commissioner need to be notified?</p> <p><i>Please indicate, the DPO will confirm when they review this form.</i></p>	
<p>Do any individuals need to be notified?</p> <p><i>Please indicate, the DPO will confirm when they review this form.</i></p>	
<p>Have you notified or are you planning to notify any other external organisations about the breach?<sup>4</sup></p>	
<p>Do we need to review or make changes to our policies or how we operate as a result of this breach?</p> <p>What lessons have been learned from this breach?</p> <p><i>Please indicate, the DPO will confirm when they review this form.</i></p>	
<p>Describe the actions you have taken, or propose to take, as a result of the breach</p> <p>Include, where appropriate, actions you have taken to fix the problem, and to mitigate any adverse effects, e.g. confirmed data sent in error has been destroyed, updated passwords, planning information security training.</p>	
<p>If there has been a delay in reporting the breach, please explain why</p>	

---

<sup>4</sup> You may need to consider notifying third parties such as the police, insurers, other regulators or supervisory authorities, or bank or credit card companies who can help reduce the risk of financial loss to individuals.

DPO Use	
Date reported to the DPO	
Entered into Central Log (Y/N)	
DPO confirms a breach has occurred (Y/N)	
Date Completed	
Completed by	
Signed off by	
Follow up	

## Appendix 4: Data Breach Procedure Flowchart

