OADBY & WIGSTON BOROUGH COUNCIL

PERSONAL DATA BREACH PLAN

Policy Version Number: 2.0
Policy Author: Data Protection Officer
Authorisation: Senior Leadership Team
Date of Next Review: May 2025

Contents

1.0 Introduction

1.1. Oadby and Wigston Borough Council have 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 processes 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.
- IT Acceptable Use Policy.
- Home and Remote Working Policy.
- CCTV Policy, Procedures and Guidelines.

All staff have also undertaken training on 'Learning Pool'.

2.0 Purpose

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

2.2 Instances of the loss of personal data are rare in the Council; however, the consequences to the reputation of the organisation and the potential impacts on individual service users of the loss of personal information 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) has the ability to impose significant fines on data controllers for serious contraventions of the UK GDPR.

2.4 The ICO also has the ability to 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.

3.0 Aim

3.1 This plan sets out the Councils' 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 their possession is kept safely and securely and that processes are in place to minimise or mitigate the impact of a personal data breach.

4.0 Roles and Responsibilities

4.1 This plan will be reviewed every three years, or earlier, if necessary.

4.2 Heads of Service will be responsible for ensuring operational compliance with this plan within their service areas and for seeking advice from the Data Protection Officer, or Information Governance Manager, when appropriate.

4.3 The Council's Data Protection Officer is responsible for the provision of advice and guidance regarding this plan.

5.0 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. Heads of Service should ensure that all staff within their responsibility are familiar with the appropriate policies and procedures.

5.3 All data controllers (the Council) have 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 as detailed below:

"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 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.

6.0 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 any of a number of 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 attack.

- Information obtained by surreptitious or deceptive means (blagging).
- Information being released inappropriately.

7.0 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.

8.0 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 officer. This should be done using the **Data Breach Incident Reporting form.**

8.2 It is recommended that a senior officer is at that point nominated as 'breach owner' and that the relevant Head of Service 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 Head of Service of the department concerned.

8.4 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. Similarly, should a breach of personal data originate from a partner organisation, 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 taken place the following information will be required in order 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 by the breach).
- 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, and financial implications?

8.6 If after the initial assessment a breach has been clearly identified then an incident response team should be co-ordinated by the relevant Head of Service. This should include the key officers involved in the breach, as well as a lawyer nominated by the Lawyer to the Council. It may also be worth alerting the Council's Communications team at this stage so they can be ready to deal with any media enquiries.

The key officers involved should be proportionate to the type of breach. For instance a minor breach may require the following:

- Line Manager
- Senior Officer (breach owner)
- Head of Law and Democracy
- Audit Officers
- Head of Service

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

- Chief Executive/Deputy Chief Executive.
- Head of Service.
- Lawyer to the Council.
- Any relevant Heads of Service

- Senior Officer within department (breach owner).
- Head of Law and Democracy
- Audit Officers

8.7 Responsibility rests with the Head of Service, or their nominated deputy, in considering the action to be taken to:

- Protect the interests of the customer.
- Ensure the continuing delivery of the service.
- Protect the interests of the Council.
- Meet the requirements of the UK GDPR in terms of informing the Information Commissioner's Office (see section 8 below).

8.8 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.

8.9 Fully assess the risk in terms of the potential adverse consequences for individuals. How serious or substantial are the consequences and how likely are they to happen?

9.0 Notifying the Information Commissioner's Office (ICO)

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

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 or not to inform the ICO would normally rest with the Head of Service. However, there may be circumstances where the decision to report the breach is the responsibility of the Chief Executive or Deputy Chief Executive e.g. where the information lost is owned by a number of services, or where the implications of the breach would seriously affect the reputation of the Council as a whole.

9.5 If the decision is to notify the ICO, the Data Protection Officer will act as liaison with the ICO. They will also ensure that the Chief Executive and Deputy Chief Executive are informed of all reported breaches.

9.6 The Head of Service in conjunction with the Head of Law and Democracy and the Head of People and Performance (Human Resources) 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:

- 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.
- Communicate the name and contact details of the Data Protection Officer or other contact point where more information can be obtained.
- Describe the likely consequences of the personal data breach.
- 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 in so far 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. That 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 up to 10 million Euros; this is at the discretion of the ICO.

How to notify the ICO:

- Online Form: https://ico.org.uk/media/for-organisations/documents/2258298/personal-data-breach-report-form-web-dpa-2018.doc
- Web page: https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/
- Telephone: 0303 123 1113

10.0 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 have been breached. Examples of such damage are:

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

10.2 When the breach involves personal 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 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 Article 29 Breach Reporting.

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, in particular 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 Officers should consider consulting 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.

11.0 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 1: Examples of Incidents

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

Malicious

- Giving information to someone who should not have access to it – verbally, in writing or electronically.
- Computer infected by a virus or similar.
- Sending a sensitive email to 'LDC All or EBC All' or unintended recipient.
- Receiving unsolicited mail of an offensive nature.
- Receiving unsolicited mail which requires you to enter personal data.
- Finding data that has been changed by an unauthorised person.
- Receiving and forwarding chain letters, including virus warnings, scam warnings and other emails which encourage the recipient to forward to others.
- Unknown people asking for information which could gain them access to council data e.g. a password or details of a third party.

Misuse

- Use of unapproved or unlicensed software on the council's equipment.
- Accessing a computer database using someone else's authorisation e.g. someone else's user id and password.
- 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.

Theft/Loss

- Theft/loss of a hard copy file.
- Theft/loss of any of the council's computer equipment.

Appendix 2: Definitions

Personal data

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

'Identifiable living individual' means a living individual that can 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

'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

'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

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

Data subject

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

Appendix 3: Examples of 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	As long as the data are 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 Council Office 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.	

Example	Notify the ICO	Notify the data subject	Notes
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 are 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 we take the additional step of notifying other individuals if there is a high risk to them.