Data Breach Policy

Document Control

Organisation	Gravesham Borough Council (GBC)
Title	Data Breach Policy
Author	Tejinderpreet Lalli, Head of Information Governance & DPO
Filename	GBC Data Breach Policy
Owner	Senior Information Risk Owner (SIRO)
Subject	Data Incidents
Protective Marking	Official/Recipients Only
Last Review date	March 2026

Revision History

Revision Date	Revisor	Previous Version	Reason for revision
October 2019	Gayle Jones (DPO)	-	Establish policy in line with GDPR & DPA 2018 – Version 1.2
May 2023	Tejinderpreet Lalli	2.0	Scheduled Review
Jan 2026	Tejinderpreet Lalli		Scheduled Review

Document Approvals

This document requires the following approvals:

Sponsor Approval	Name	Date
Senior Information Risk Officer (SIRO)	Sarah Parfitt, Director (Corporate Services)	
Management Team	Stuart Bobby, Chief Executive	

Document Distribution

This document will be distributed to:

Name	Job Title	Email Address
All council employees who handle personal data and Elected Members	All job titles	Via agreed process
All employees of shared services commissioned by the council who handle personal data of which GBC is the data controller.	All job titles	Via agreed process.
Publication on the council's website and staff intranet	N/A	Via Digital Team

Contributors

Development of this policy was assisted through information provided by the following organisations:

Kent County Council

Contents

Busy reader's summary....4
1. Introduction and Objectives....5
2. Scope....5
3. Roles and responsibilities....5
4. What is a personal data breach and how to report the breach or incident....6
5. Action to take on discovery of the breach....7
6. Managing and recording the breach....7
7. Notification to appropriate parties of the breach....8
8. Notifying the ICO....8
9. Notifying data subjects....8
10. Notifying the Police and other parties....9
11. Preventing future breaches....9
12. Monitoring and review....10
13. Staff awareness and training....10
14. Consequences of non-compliance....10
15. Guidance....10
16. Review....10
Appendix 1: Cyber Response: IT and Information Governance (IG) Collaboration....11

Busy reader's summary

- This policy applies to all the personal information held by Gravesham Borough Council, its subsidiaries, and its contractors.
- **A** personal data breach **is a security risk that affects** personal data **in some way.**
- A personal data breach may put data subjects' rights and freedoms at risk. This can include physical, material, or non-material risks.
- Examples are identity theft, fraud, and other financial loss. Other cases include damage to reputation or social disadvantage.
- In the event of a suspected personal data or information security breach: DO NOT WAIT – ACT and REPORT ANY INCIDENTS IMMEDIATELY to the Information Governance team (gdpr@medway.gov.uk)
- **If a breach occurs, Gravesham Borough Council must take certain steps to manage the breach.**
- Gravesham Borough Council must report a 'high risk' data breach to the Information Commissioners Office (ICO) within 72 hours.
- The member of staff reporting the breach, or any other person should not take any further action in relation to the breach without consulting with the Information Governance team. He or she must not notify any affected individuals or regulators.

1. Introduction and Objectives

1.1 Any information that could identify a living individual (directly or indirectly) is classed as personal data. GBC is required, under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA18), to implement appropriate technical and organisational measures that ensure the appropriate security of the personal data it processes as the 'Data Controller'.

1.2 GBC is committed to managing personal data in a fair, transparent and lawful way. It will ensure the security and integrity of information, particularly personal data and sensitive personal data by implementing and maintaining appropriate controls and procedures for its handling and storage.

1.3 GBC must ensure that personal data is processed in a manner that ensures appropriate protection from unauthorised and unlawful processing and from accidental loss, destruction or damage.

1.4 Part of that commitment is to ensure that appropriate steps are taken in the event of a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

1.5 Whilst instances of the loss of personal data are rare, the consequences to GBC's reputation and the potential impact on the individuals whose data is breached (whether they are service users or employees) means that it is essential to take swift and appropriate action in the event of a data breach. to:

1.6 The Information Commissioner's Office (ICO) has the ability to impose significant fines of up to £17 million or 4% of the organisation's annual global turnover (whichever is higher) on data controllers for serious contraventions of the GDPR. The commissioner can also serve an enforcement notice on data controllers if it considers positive steps are necessary to bring about compliance.

2. Scope

2.1 The policy applies to all GBC staff and volunteers and, through contractual arrangements with GBC, suppliers, partners, partners, contractors, agents, consultants and commissioned services, in the course of functions carried out for or on behalf of - other councils under the shared service agreement.

2.2 This policy sets out the steps that must be followed in the event of data loss, theft or uncontrolled exposure of personal or sensitive information for which GBC has responsibility. This policy also acknowledges risks related to failing to protect personal information, which can include financial loss, damage to reputation and colleague morale, and most importantly, distress and harm to people.

2.3 Personal data breaches may involve criminal or civil liability, or both, depending on the circumstances, and may include both individual and corporate responsibility.

2.4 Throughout this document, the term 'information' refers to personal data or to information that is commercial or political information of a sensitive/confidential nature.

2.5 Computerised equipment, for the purposes of this policy, includes, but is not limited to personal computers (PCs – laptops, notebooks, tablets and smartphones, application servers, file/print servers) and mobile phones. It also includes all types of removable storage media; peripheral devices and/ accessories physically attached, or connected by wireless networks, to the computerised equipment.

3. Roles and responsibilities

3.1 The Senior Information Risk Owner (SIRO) has overall responsibility for this policy. This policy will be reviewed every 2 years, or earlier if necessary.

3.2 Directorates are responsible for ensuring operational compliance with this policy within their service areas and for seeking advice either directly from the Data Protection Officer or the Information Governance Team (IG).

3.3 Elected members are data controllers in their own right and are subject to the same legal obligations as the Council. In addition, members (elected Councillors) are bound by obligations under the Members' Code of Conduct but must also be aware of their corporate and personal responsibilities to understand the requirements of the GDPR and to act in response to any breaches in relation to personal data.

3.4 All staff must be aware of their responsibilities for handling personal data, keeping it secure and not disclosing it without authorization. Personal information must only be used for the purpose for which it was obtained and must not be misused. Managers must ensure that staff are familiar with the appropriate policies, including the Data Protection and Information Security policies, and complete the mandatory Information Governance and GDPR training courses as relevant.

3.5 Anyone who handles personal or sensitive information for and/or on behalf of GBC must:

- Take all reasonable steps to ensure the security of that information to minimise the risk of a data breach, including the loss of personal or sensitive information;
- Be familiar with GBC's Data Protection and Information Security Policies;
- Follow the procedure outlined below in the event of any breach of security.

4. What is a personal data breach and how to report the breach or incident

4.1 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 personal data breach is not limited to just losing personal data.

4.2 A personal data breach can happen in a number of ways for various reasons:

- Loss or theft of data or equipment which holds personal data e.g. laptops, tablets, USB drives, CDs or paper copies, CCTV or surveillance equipment
- Equipment failure
- Inappropriate access controls allowing unauthorised use
- Human error (such as sending an email to the wrong recipient)
- Hacking, phishing or blagging (information obtained by deception)
- Unforeseen incidents such as fire or flood.

4.3 In the event of a suspected personal data or information security breach: **DO NOT WAIT – ACT and REPORT ANY INCIDENTS INTERNALLY IMMEDIATELY**

4.4 It is crucial to act quickly in the event of a data breach or suspected information security incident, in order to minimise the impact of the incident and safeguard the privacy of individuals as far as possible and minimise the risk to GBC.

4.5 The initial steps that should be taken to alert managers about an incident will vary depending on whether the incident involved a member of GBC staff, a supplier or commissioned service, a service user or member of the public or an elected Member. If your manager is absent, do not wait for their return, contact the Information Governance team immediately.

4.6 A data incident notification form (link here) must be completed immediately and sent to Information Governance team: gdpr@medway.gov.uk containing 'Data Breach', 'DPA Incident' or 'Security breach' in the subject line. This must be sent within 24 hours of 'becoming aware' of the data breach or security incident.

4.7 GBC is required under the GDPR to notify the ICO when a personal data breach is likely to result in a risk to the rights and freedoms of the Data Subjects whose data has been breached. Where the ICO notification is required, this must be made within 72 hours of 'becoming aware' of the incident/breach.

5. Action to take on discovery of the breach

5.1 If an information breach has occurred or you have been made aware, the officer or other person concerned should:

- where possible, retrieve any lost equipment or papers
- where theft or the loss of sensitive information which could risk the safety of others is involved, report the incident to Heads of Service who should then report it to the police with all relevant details
- Notify their manager/a GBC member of staff as follows:
  (i) Employees and contract workers should notify their line manager, or (if unavailable) the next senior manager. In their absence contact the Information Governance team.
  (ii) Suppliers of commissioned services (sometimes referred to as 'Data Processors') should inform their GBC contract manager.
  (iii) Where a data breach is reported to the customer contact centre by a member of the public, the contact centre must inform Information Governance team (gdpr@medway.gov.uk), who will refer the incident to the relevant head of service.
  (iv) Elected members who identify a breach relating to their role within the council (not as a representative of their ward or political party) should initially contact the head of service or director concerned.
- Report the loss of any IT equipment or an electronic security breach to the IT Service Desk. Where the security breach or suspected security breach involves PSN data, this must be reported to the PSN immediately via IT Services. Appendix 1 details the incident response plan when such incident occurs.
- Complete a data incident report form, in liaison with the employee's line manager if necessary.
- Email the completed form to gdpr@medway.gov.uk. An anonymous report can be submitted by a non-electronic method, e.g. internal post to the IG Team or the DPO.

5.2 The officer or other person should not take any further action in relation to the breach. He or she must not notify any affected individuals or regulators.

5.3 The IG team will:

- acknowledge receipt of the data incident report

(a) log the breach in the security incident log;

(b) take appropriate steps or provide guidance to mitigate/manage risks associated with the breach.

5.4 The person discovering (or the manager being informed) of the potential breach must not personally contact the Information Commissioner's Office.

6. Managing and recording the breach

6.1 The Information Governance team in consultation with the service area and SIRO will take immediate steps to establish whether a personal data breach has, in fact, occurred. If so, they will take appropriate action to:

- Investigate and contain the data breach and (so far as reasonably practicable) recover, rectify or delete the data that has been lost, damaged or disclosed (subject to any requirements to preserve potential evidence)
- Identify how the breach occurred and take immediate steps to stop or minimise the further loss, destruction or unauthorised disclosure of personal data
- Assess and record the breach in GBC's data breach register
- Notify appropriate parties of the breach and inform them what they must do (this could be finding lost equipment, isolating or closing part of the network or changing passwords)

- Fully assess the risk in terms of the potential adverse consequences for individuals: how serious are the consequences and how likely are they to happen?
- - Provide advice to prevent further breaches/recurrences and record learning from the incident.

7. Notification to appropriate parties of the breach

7.1 It might be necessary to notify the following parties:

- The ICO
- Affected data subjects
- The Police
- The PSN (Public Service Network) team
- The NCSC (National Cyber Security Centre) (where applicable)
- Any other parties e.g. insurers or commercial partners

7.2 Ultimately the decision whether to notify lies with - SIRO in liaison with the DPO, particularly where the implications of the breach would seriously affect GBC's reputation.

8. Notifying the ICO

8.1 GBC is required under the GDPR to notify the ICO when a personal data breach has occurred if the personal data breach is likely to result in a risk to the rights and freedoms of data subjects. By- risk it means, but is not limited to:

- discrimination
- damage to reputation
- financial loss
- loss of confidentiality
- or any other significant economic or social disadvantage.

8.2 Where ICO notification is required, this shall be done without undue delay and, where feasible, not later than 72 hours after having become aware of it. Where the notification to the ICO is not made within 72 hours, it will be accompanied by reasons for the delay. The DPO/IG team will notify the ICO on behalf of SIRO and service area.

8.3 Any notification to the ICO must:

- 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 DPO or other contact who can provide information.
- Describe the likely consequences of the personal data breach.
- Describe the measures taken or proposed to be taken by GBC to address the personal data breach, including, where appropriate, measures to mitigate any possible adverse effects.

8.4 If all the information is not available within 72 hours this information may be provided in phases, provided further information is provided to the ICO without undue delay.

8.5 It is the sole responsibility of the information governance team to make contact (if appropriate) with the ICO.

9. Notifying data subjects

9.1 Where the data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Head of service in consultation with SIRO will notify the affected individual(s) without undue delay.

9.2 Any notification must include:

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

- The likely consequences of the personal data breach
- The measures GBC has taken or intends to take to address the personal data breach, including, where appropriate, recommendations for mitigating potential adverse effects.

9.3 When determining whether and how to notify data subjects of the breach, GBC will:

- Co-operate closely with the ICO (consulting it about how to inform data subjects if necessary)
- And other relevant authorities, e.g. the police

9.4 In some circumstances, service users are vulnerable adults and children and being informed of a security incident may be alarming. In these circumstances the Director or their nominated deputy will consider appropriate communication strategies.

9.5 It may be important to point out at an early stage of a security incident (rather than a confirmed breach) that there is no indication that their personal security has been breached but the members of the public must remain vigilant and will be advised of any change in security status. If any of the information relates to personal finances details, then the individual should be advised to contact their bank or building society urgently and to monitor their bank/building society account(s).

9.6 The Director or nominated deputy will need to authorise a briefing for all the necessary parties within a single email, blind copied (BCC) to the appropriate contacts. Depending on the potential seriousness of the security breach, contact is advised by phone as well as face to face. Any significant change to status will require follow-up communication.

10. Notifying the Police and other parties

10.1 The DPO in consultation with SIRO will already have considered whether to contact the police for the purpose of containment and recovery. Regardless of this, if it subsequently transpires that the breach arose from a criminal act perpetrated against or by a representative of GBC, the - Head of service will notify the police and/or relevant law enforcement.

10.2 The Head of service will consider whether there are any legal or contractual requirements to notify any other parties, e.g. in compliance with a contract or a data sharing agreement.

11. Preventing future breaches

11.1 Once the personal data breach has been dealt with, in accordance with this plan, the Information Governance team will:

- Establish what security measures were in place when the breach occurred
- Assess whether technical or organisational measures can be implemented to prevent the breach happening again
- Consider whether there is adequate staff awareness of security issues and address any gaps through training, tailored advice or capability
- Consider the outcome of any investigations into the cause of the breach and whether action should be taken under GBC's disciplinary procedure
- Consider whether it is necessary to update GBC's privacy risk assessments or Data Protection Impact Assessments.
- Update GBC's risk register, and Data Breach Register with the facts of the breach, its effects and the remedial action taken.

11.2 A security incident must remain in the 'OPEN' status, until finally resolved and only 'CLOSED' after it has been resolved, reviewed and any requirements for training, disciplinary and/or procedural changes have been identified. The cases will be closed by the Information Governance team.

12. Monitoring and review

12.1 GBC will monitor the effectiveness of all its policies and procedures regularly, and conduct a full review and update as appropriate, at least annually.

12.2 GBC's monitoring and review exercises will include looking at how its policies and procedures are working in practice to reduce the risks posed to the council.

13. Staff awareness and training

13.1 Key to the success of GBC's systems is its staff awareness and understanding.

13.2 GBC provides regular training to staff:

- at induction
- on an ongoing basis as this must be refreshed every year
- when there is any change to the law, regulation or the policy
- when significant new threats are identified
- in the event of an incident affecting the council or its service users.

14. Consequences of non-compliance

14.1 Failure to comply with this policy and associated policies (e.g. GBC's Data Protection or Information Security Policies) puts individuals and GBC at risk.

14.2 Failure to notify the DPO or IG of an actual or suspected personal data breach is a very serious issue.

14.3 A failure to comply with this policy by:

- GBC employees: may result in disciplinary action and may, in cases of Gross Misconduct (including negligence), result in termination of employment
- GBC Members: may be referred to the Standards Committee, which can recommend disciplinary measures to the Council
- Third Parties: (agents, contractors and consultants) engaged to carry out work for and on behalf of Gravesham Borough Council: may result in the termination of the contract and/or litigation.

15. Guidance

15.1 If staff, suppliers or members do not understand this policy or if more details are needed regarding any of the steps or staff and others' responsibilities then contact GBCs:

- Data Protection Officer and Information Governance Team: gdpr@medway.gov.uk
- Advice on Information Security and Information Risk Management can be obtained by contacting the IT Services.

16. Review

16.1 The policy will be reviewed by the Information Governance & Security Group (IGSG) every 2 years. In addition, changes to legislation, codes of practice or commissioner may trigger interim reviews.

Appendix 1: Cyber Response: IT and Information Governance (IG) Collaboration

During cyber-attacks such as ransomware (an electronic security breach) or phishing (obtaining information by deception), Gravesham Borough Council (GBC) requires a coordinated response between the IT Services and Information Governance (IG) teams to mitigate both technical and regulatory risks.

1. Incident Discovery and Joint Reporting
    - Immediate Notification: Any member of staff who suspects a phishing attempt has compromised data or that a ransomware attack is underway must not wait and must report the incident immediately.
    - Dual Reporting Lines: Electronic security breaches must be reported to the IT Service Desk and simultaneously to the IG team via gdpr@medway.gov.uk. If the breach involves Public Service Network (PSN) data, it must be reported to the PSN immediately through IT Services.
    - Internal Deadlines: A data incident notification form must be sent to the IG team within 24 hours of becoming aware of the incident.
2. Containment and Technical Isolation
    - IT Lead: IT Services are responsible for the technical containment of the attack, which may include isolating or closing parts of the network, changing passwords, or finding and securing compromised equipment.
    - IG Lead: While IT secures the infrastructure, the IG team provides guidance on mitigating and managing the risks associated specifically with the personal data involved in the breach.
    - Evidence Preservation: Both teams must work to recover or delete lost/disclosed data while adhering to requirements to preserve potential evidence for further investigation.
3. Coordinated Investigation and Risk Assessment
    - Determining the Breach: The IG team, in consultation with IT and the relevant service area, establishes whether a formal personal data breach has occurred (e.g., accidental or unlawful destruction, loss, or unauthorised access to data).
    - Technical Forensics: IT provides the technical details of the "hacking" or "phishing" event, while IG assesses the potential adverse consequences for individuals, such as identity theft, fraud, or damage to reputation.
    - Categorisation: IT and IG collaborate to identify the categories and approximate number of data subjects and records concerned, which is a mandatory requirement for regulatory reporting.
4. External Notification Duties
    - ICO Reporting: If the incident is deemed "high risk" to the rights and freedoms of individuals, the IG team (on behalf of the SIRO) must notify the Information Commissioner’s Office (ICO) within 72 hours.
    - Regulatory Liaison: IT Services provide the necessary technical information to the IG team to describe the measures GBC has taken (or proposes to take) to address the breach and mitigate its effects.
    - Other Parties: The IG team and the Head of Service determine if other bodies need notification, such as the Police, the National Cyber Security Centre (NCSC), or the PSN team.
5. Post-Attack Mitigation and Prevention
    - Closing the Incident: A security incident remains "OPEN" until IT and IG confirm it is resolved and all training or procedural changes are identified.

- Future Safeguards: Following the attack, the IG team evaluates the security measures that were in place and works with IT to implement new technical or organisational measures to prevent a recurrence.
- Risk Updates: IG updates the Council's Data Breach Register and risk assessments, while IT provides advice on ongoing Information Security and Information Risk Management.