Data Breach Procedure

#### Version 2.0

#### January 2023



|  |  |  |  |
| --- | --- | --- | --- |
| **Owner (Responsible for Approval of Issued Versions)** | | | |
| Kit Collingwood – Assistant Director of Digital and Access and Senior Information Risk Owner (SIRO) |  |  |  |
| David White – Head of Information, Safety and Communities and Data  Protection Officer |  |  |  |

##### Revision History:

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Reason for change** | **Author** |
| 19 February 2018 | 0.1 | New Procedure in line with DP 2018 | Marsha White |
| 16 April 2018 | 0.2 | Modified following comments from IGWG and Legal | Marsha White |
| 10 May 2018 | 0.3 | Added roles and responsibilities and flow chart | Louise Morris |
| 21 May 2018 | 0.4 | Revisions with Children Services | Gerard Murphy |
| 07 June 2018 | 0.5 | Revisions with Knowledge Information Manager | Doug Plumer |
| 19 June 2018 | 1.0 | Final Version Approved by DPO | Marsha White |
| 25 May 2022 | 1.1 | Updates to Procedure | Ayomide Adediran |
| 20 July 2022 | 1.2 | Modified following comments from IGWG and Legal | Ayomide Adediran |
| 18 January 2023 | 2.0 | Approved by DPO | David White |

##### Distribution:

|  |  |  |
| --- | --- | --- |
| **Date** | **Version** | **Distribution** |
| 19 June 2018 | 1.0 |  |
| 23 January 2023 | 2.0 |  |

### TABLE OF CONTENTS

[1 Introduction 5](#_Toc125378071)

[2 Policy Statement 6](#_Toc125378072)

[3 Aims and Objectives 6](#_Toc125378073)

[4 Roles and Responsibilities 6](#_Toc125378074)

[5 Definitions 8](#_Toc125378075)

[6 Training 9](#_Toc125378076)

[7 Identification 9](#_Toc125378077)

[8 Investigation 10](#_Toc125378078)

[9 Risk Assessment 11](#_Toc125378079)

[10 Containment and Recovery 11](#_Toc125378080)

[11 Informing Individuals Affected 12](#_Toc125378081)

[12 Sharing and Learning 13](#_Toc125378082)

[13 Performance Monitoring Responsibilities 13](#_Toc125378083)

[14 Information Governance Working Group 13](#_Toc125378084)

[15 Data Breach Log 13](#_Toc125378085)

[16 Appendices 14](#_Toc125378086)

Greenwich

## **Introduction**

* 1. The UK General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA) are underpinned by seven principles:
     + first data protection principle – processing must be lawful, fair and transparent;
     + second data protection principle – purposes of processing must be specified, explicit and legitimate;
     + third data protection principle – personal data must be adequate, relevant and not excessive;
     + fourth data protection principle – personal data must be accurate and kept up to date;
     + fifth data protection principle – personal data must be kept for no longer than is necessary;
     + sixth data protection principle – personal data must be processed in a secure manner; and
     + seventh data protection principle – the controller should be able to demonstrate compliance with the above six principles (accountability)
  2. These give individuals specific rights in relation to their personal information and place certain obligations on organisations that are responsible for processing it. An overview of the main provisions of DPA can be found in the Guide to Data Protection: [https://ico.org.uk/for-](https://ico.org.uk/for-organisations/guide-to-data-protection) [organisations/guide-to-data-protection.](https://ico.org.uk/for-organisations/guide-to-data-protection)
  3. Occasionally things may go wrong and mistakes may be made. Sometimes this may entail significant financial or reputational risk for both Royal Borough of Greenwich (RBG) and our customers. It is vital that we can identify, evaluate, and contain data breaches as soon as they occur and within 72 hours, where feasible.
  4. Consistent governance and control arrangements are also a regulatory requirement. Where a breach has occurred and/or where we have failed to mitigate the impact quickly, the Information Commissioner (ICO) may intervene and may use its powers to issue a substantial fine.
  5. Identifying data breaches quickly and effectively to limit any impact on our customers is critical to our success in mitigating the impact of the breach. Equally we need to understand areas of weaknesses within our operating processes and continuously improving to reduce the risk of significant control failures leading to data breaches.
  6. This procedure meets the guidance provided by the ICO on data security breach management.

## **Policy Statement**

* 1. The Procedure is in place to raise awareness of data breach cases and to ensure that all staff and managers can identify a case and understand the steps required for dealing with them.
  2. The procedure identifies inherent risk of a data breach and/or near-miss, which will ensure that appropriate senior management is informed, able to manage actions relating to any real or potential serious data breach and be in a position to report to the ICO and affected individuals as appropriate.

## **Aims and Objectives**

* 1. This procedure sets out:
     + Our policy statement on data breaches
     + Roles and responsibilities
     + The process for handling data breaches.
  2. This procedure aims to ensure that adequate controls are in place so that:
     + Data breaches are identified and action is taken quickly. Actions must be proportionate, consistent, and transparent
     + An assessment is completed by the Investigating Manager. With support from the Departmental Information Governance Representative (DIGR), the Investigating Manager is to ensure that any high risk data breaches are reported to the Data Protection Team and Data Protection Officer (DPO). All data breaches and near misses are recorded and regularly reported.
     + Lessons are shared and learnt to ensure similar mistakes are not repeated and appropriate control mechanisms are put in place.

## **Roles and Responsibilities**

|  |  |
| --- | --- |
| **Roles and responsibilities** | |
| **Role** | **Responsibility** |
| Officer who discovers the breach / near miss (Reporting Officer) | * Any member of staff that initially identifies a breach/potential breach/near miss. * Reports the matter to their line manager * Completes the incident form and risk matrix |
| Investigating Manager | * Manager of reporting officer (i.e. Team Leader or Head of Service) * Carries out initial ‘triage’ of risk and reports this immediately to an identified Data Owner and Departmental Information Governance Representative (DIGR) *this report may be made*   *directly or through their immediate line management.* |
| Data Owner  (the Head of the Service  that is most directly responsible for holding the  data in question, or a nominated person) | * Will initiate the breach management process concentrating on   1. Containment and recovery   2. Assessment of on-going risk * May undertake tasks directly or lead the task with other officers |
| Departmental Information Governance representative (DIGR) | * Directorate lead for advice and guidance * Will inform the Director / Snr AD. * Consult with the Caldicott Guardian – if appropriate * Lead on seeking legal advice   Member of the Information Governance Working Group |
| Information Governance Manager | * Provides advice and support to DIGR * Reviews data protection incident documentation * Supports investigation process |
| Data Protection Lawyer | * Provides legal advice * Works alongside Information Governance Manager |
| Data Protection Officer | * Decision making point for determining reportable personal data breaches (UK GDPR) to the ICO. * Decision making point for determining reportable Privacy and Electronic Communications Regulations (PECR) breaches to the ICO.   Liaising with ICO and external partners. |
| Information Governance Working Group | Members will review and cascade lessons learnt to inform changes to practice, and actions required to prevent future breaches |
| Steering group | Receive a high level / annual report on data breaches and follow up actions |
| SIRO | * Decision making point for determining reportable PECR breaches to the ICO.   Monitoring the investigation |
| Information Commissioners Office (ICO) | * The Information Commissioner’s Office (ICO) upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.   ICO is an executive non-departmental public body, sponsored by the Department for Digital, Culture, Media & Sport. |

## **Definitions**

##### What is a personal data breach?

* + 1. According to the ICO, organisations which process personal data must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data.
    2. A data breach is “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”.

* + 1. A personal data breach may mean that someone outside RBG gets unauthorised access to personal and/or special category (sensitive) data. A personal data breach can also occur if there is unauthorised access within RBG, for example, an employee **accidentally** or deliberately alters or deletes personal data.
    2. A data breach can happen for many reasons:
       - Loss or theft of data or equipment on which data is stored
       - Inappropriate access controls allowing unauthorised use
       - Equipment failure resulting in a loss or data being exposed to unauthorised parties
       - Human error e.g. emailing information to the wrong person
       - Unforeseen circumstances such as a fire or flood damaging records
       - Cyber attack
       - ‘Blagging’ offences where information is obtained by deceiving the organisation who holds it.
       - Failure to undertake adequate verification checks

5.1.5 Human error is the most common cause of data breaches. These can happen for many reasons:

* + - * Loss of paperwork
      * Data posted/emailed to incorrect address and/or recipient
      * Failure to correctly redact 3rd party information when disclosing information e.g. SARs or sharing an un-redacted report containing personal/sensitive data.
      * Failure to use blind carbon copy and exposing recipient’s email addresses

##### What is a near miss?

* + 1. A near miss is an event which does not result in a data breach but had the potential to do so. Examples of such events might include data that was misplaced but found quickly internally or data that was sent out but was identified and returned.
    2. The Council is committed to identify weaknesses in its procedures. All near misses will be recorded by the DIGR in order to understand patterns, learn lessons and implement improvements. Near misses are important to learn from, as they can help identify weakness without the legal, financial and other risks that result from a breach.
  1. **What is PECR?** 
     1. The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) provide rules about sending marketing and advertising by electronic means, such as by telephone, fax, email, text and picture or video message, or by using an automated calling system. PECR also include other rules relating to cookies, telephone directories, traffic data, location data and security breaches.
     2. More information on PECR can be found [here](https://ico.org.uk/for-organisations/guide-to-pecr/). Some examples of a PECR breach include:
* Use of electronic mail for direct marketing purposes
* Making unsolicited calls for direct marketing purposes

## **Training**

* 1. All staff are required to complete mandatory data protection and cybersecurity training.
  2. Training will be provided to all new employees including agency and contracted staff.
  3. All employees will undertake refresher training annually.
  4. The Information Governance Working Group representatives and other key personnel will

receive training on data breach management and data breach reporting.

* 1. Training will be audited and reported to the Information Governance Steering Group.

# Identification

* 1. Data breaches or near misses may be identified as part of everyday business monitoring and reporting. They may be identified by the Contact Centre at the first point of contact or by our contractors, or staff via discussions in team meetings, during individual 121 meetings, through the analysis of performance information, from customer complaints, or as part of wider service improvement work. They may also be identified via a whistle blowing case.
  2. All incidents must be reported. Where an incident has emerged, a data protection incident form (Appendix A) and risk assessment matrix (Appendix B) would need to be completed by the reporting officer and must be sent by email to [data.protection@royalgreenwich.gov.uk.](mailto:data.protection@royalgreenwich.gov.uk.%20)
  3. The Investigating Manager (with support from the DIGR) will investigate the occurrence.
  4. The controls in place must be reviewed. Where no controls are in place, consideration must be given to introducing them. A question could be, “w*as this an exceptional case that could not have reasonably been avoided, or does action need to be taken to avoid a recurrence?”*

# Investigation

* 1. A formal investigation must be commenced by the Investigating Manager who must determine the seriousness of the breach and the risks arising from it. Specifically, they must identify:
     + Whose information was involved in the breach
     + What went wrong
     + The potential effect on the data subject(s)
     + What immediate steps are required to remedy the situation
     + What lessons have been learnt to avoid a repeat incident
     + In order to support this process, all sections of the data protection incident form template must be completed (Appendix A).
  2. The investigation must consider:
     + The type of information
     + Its sensitivity
     + How many individuals are affected by the breach?
     + What protections are in place (e.g. encryption)?
     + What happened to the information?
     + Whether the information could be put to any illegal or inappropriate use
     + What could the information tell a third party about the individual?
     + How many people are affected?
     + What types of people have been affected (the public, suppliers, staff etc)?
     + Whether those affected have any special needs/vulnerabilities.

NOTE: Actions to contain and recover data as well as mitigate any risk must be taken immediately. The Investigating Manager is to ensure that the case is being managed and any improvement actions agreed are implemented. The investigation must be proportionate to the breach identified and risk of harm.

* 1. The initial investigation must be completed urgently and wherever possible within 24 hours of the breach being discovered / reported – this may be a partial response which can be updated once more information has been identified. A further review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.
  2. However, some level of investigation might be required to carry out the Risk Assessment Matrix (Appendix B) and determine the most appropriate route of escalation. If, once identified, risk of a data breach is contained and does not pose immediate further threat to the business and/or customers, timeframes for official escalation/notification can be extended to allow for a more thorough investigation. Extensions must be agreed at each stage and noted in the data protection incident form (Appendix A).
  3. As an investigation proceeds the risk may change and the reporting requirements must be amended in line with the change in risk. For example, a case identified as a medium risk initially may increase to a high risk and therefore must be escalated to the DPO or SIRO (depending on the type of breach).
  4. Advice, input and support can be sought from other sources (DIGR, Information Governance Team, Corporate ICT etc.) as required.

# Risk Assessment

* 1. When a data breach is identified, the Reporting Officer, with support from the Investigating Manager and DIGR must complete a risk assessment using the Risk Assessment Matrix (Appendix B).
  2. Depending on the risk assessment score, the data breach will be reported to, owned and investigated at the specified levels within the organisation referring to the Reporting/Escalation Mechanism (Appendix B).
  3. The Data Protection Officer, Information Governance Manager and DIGR will be made available to support the data breach Investigating Manager. The Data Protection Officer or Information Governance Manager will provide advice and guidance on managing the containment and recovery of any lost data and will support the investigation process. However, ownership of the breach will still be retained according to specific level identified on Appendix B.
  4. The Data Incident Process Map is attached (Appendix C) and must be used to work through the stages.

# Containment and Recovery

* 1. Containment and recovery involves limiting the scope and impact of the data breach, and containing it as quickly as possible.
  2. The Investigating Manager, with support from the DIGR and Information Governance Manager, must quickly take appropriate steps to ascertain full details of the breach, determine whether the breach is still occurring, recover any losses and limit the damage. Steps might include:
     + Attempting to recover any lost equipment or personal information.
     + Shutting down an IT system – **if appropriate**
     + Contacting the Communication team / Contact Centre and other key departments so that they are prepared for any potentially inappropriate enquiries about the affected data subjects
     + If press enquiries are anticipated, the DIGR or Data Owner must alert the Director who will inform the Chief Executive / Lead Member / Leader.
     + The DIGR or Data Owner will draft a statement for the Director to clear. This will then be passed to Communications who will seek the appropriate clearance (normally the Leader)
     + The use of back-ups to restore lost, damaged or stolen information
     + If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use
     + If the data breach includes any entry codes or passwords then these codes must be changed immediately, and the relevant organisations and members of staff informed.

# Informing Individuals Affected

* 1. The ICO requires us to inform those affected where there is a significant breach of personal

and sensitive data and the risk of harm to those individuals is high.

* 1. Clearly if there was a high risk of further harm, the Council has an obligation to disclose the breach to each individual affected. However, this has to be balanced against the risk of causing further distress and anxiety to the families by informing them about the breach.
  2. The ICO guidance states that “informing people about a breach is not an end in itself. Notification must have a clear purpose, whether this is to enable individuals who may have been affected to take steps to protect themselves or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints.”
  3. The Investigating Manager or Data Owner may decide whether to advise affected individuals of a data breach. The reasons for deciding to do this must be clearly set out in the Data Protection Incident Report. The DPO and/or SIRO may also decide whether affected individuals may need to be informed where there is a high risk to data subjects.
  4. Further advice on whether to disclose to individuals is contained in the Data Breach Guidance on Disclosure to Individuals (Appendix D).

# Sharing and Learning

* 1. An action plan for learning from data breaches and near misses must be completed and will form part of the investigation process. A lessons learnt action plan is within the Data Protection Incident Form (Appendix A).
  2. The action plan must clearly outline the lessons learnt. The controls agreed to reduce the risk of a further reoccurrence, a lead officer and a completion date.
  3. The case will not be considered closed until all actions agreed have been completed.

# Performance Monitoring Responsibilities

* 1. Investigations must be completed within 10 working days of the data breach being identified.
  2. Where a high risk has been identified:
     + An interim report must be presented to DPO, Information Governance Manager and Data Protection Lawyer within 24 hours as a minimum even when the case cannot be concluded within this timescale.
     + Updates will be sent to the Information Governance Steering Group as required.

# Information Governance Working Group

* 1. The Information Governance Working Group is a resource that can be utilised to support

investigations into identified data breaches.

# Data Breach Log

* 1. All data breaches, including near misses, will be recorded on the data breach log held centrally. All issues identified by the application of this policy will be recorded in the data breach log and categorised according to whether it is a data breach or near miss.
  2. This information will be reviewed and analysed at least monthly to identify patterns and monitor the implementation of agreed service improvements.
  3. The Information Governance Manager will collate all data breach reports through Information Governance Working Group meetings and will report trends and lessons learnt quarterly to the Information Governance Steering Group.
  4. Reference to data breaches will be included in ICT & Customer Services Annual Report.

# Appendices

Appendix A – Data Protection Incident Form



Appendix B – Risk Assessment Matrix



Appendix C – Data Incident Process Map – Flow Chart



Appendix D – Data Breach Guidance on Disclosure to Individuals

