DATA BREACH RESPONSE AND NOTIFICATION PROCEDURE

Version history

Date	Version	Created by	Description of change
18th May 2018	1.0	Data Breach Response Team	1st adopted version
25th September 2018	1.01	Michael Hynes	Final Draft

Scope, purpose and users

This Procedure provides general principles and approach model to respond to, and mitigate breaches of personal data (a "personal data breach")

The Procedure lays out the general principles and actions for successfully managing a data breach as well as fulfilling the obligations surrounding the notification to the Information Commissioner's Office (ICO) and individuals as required by the General Data Protection Regulation (GDPR).

All employees, contractors, temporary staff, volunteers and other contracted third parties working for or acting on behalf of Guildford Borough Council (GBC) must adhere to and follow this Procedure in the event of a personal data breach.

• Reference documents

- General Data Protection Regulation 2016 (Regulation (EU) 2016/679)(repealing Directive 95/46/EC))
- GBC Data Protection Policy
- GBC Acceptable Use of IT Policy
- GBC Information Systems Security Policy

- **Definitions**

The following definitions used in this document are drawn from the GDPR:

"Personal Data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person Regulation.

"Controller" is the natural or legal person, public authority, agency or any other body, which alone or jointly with others, determines the purposes and means of the processing of personal data.

"Processor" is a natural or legal person, public authority, agency or any other body which processes personal data on behalf of a Data Controller.

"Processing" means any operation or set of operations which is performed on personal data or sets of personal data, whether by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"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.

"Supervisory Authority" means an independent public authority, which is established by a Member State pursuant to Article 51. (In the UK this is the Information Commissioner's Office, ICO)

Data Breach Response Team

The Council's Data Breach Response Team ('Team') is a multi-disciplinary team comprised of knowledgeable and skilled individuals from the ICT Department (IT Security) and Legal Services. This team comprises of the Data Protection Officer (DPO), Information Rights Officer (IRO) and the Information Assurance Manager. You can contact the Team in person at the Council offices or via email at DPO@guildford.gov.uk. This Team will respond to any suspected/alleged personal data breach.

The Team ensures the necessary readiness for a personal data breach response exists, along with the procedures and guidance on best practice.

The Team will provide you with an immediate, effective, and skilful response to any suspected/alleged or actual personal data breaches affecting the Council. If required, the Team members may also involve external parties

The DPO can choose to add additional personnel to the Team for the purposes of dealing with a specific personal data breach notification.

The team will respond to a suspected/alleged or actual personal data breach notification promptly. Notification must be communicated either verbally to a member of the Team or in writing via DPO@guildford.gov.uk. If you give the notification verbally, you must follow this up with a written notification. Please refer to the notification procedure below.

Data Breach Response Team duties

Once a personal data breach is reported to the Team, the Team will carry out the following actions:

- Validate the personal data breach
- Ensure a proper and impartial investigation is initiated, conducted, documented, and concluded
- Ensure that you are advised of how to properly notify impacted data subjects, if necessary
- Report breach to the ICO within 72 hours of notification
- Identify remediation requirements and track the resolution
- Record the data breach
- Formally report findings to the Council's Corporate Management Team and Corporate Governance Standards Committee annually

Data Breach Response process

The Data Breach Response Process begins when anyone who notices that a suspected/alleged or actual personal data breach occurs, notifies any member of the Team. The Team must determine whether a breach has occurred and if so, follow the relevant procedures and processes. The Team will document all decisions ensuring traceability and accountability.

Personal data breach notification: Data processor to data controller

When the personal data breach or suspected data breach affects data that is being processed on behalf of a third party, the Council's Data Protection Officer must report any such breach to the respective data controller/controllers without undue delay.

The Team will send Notification to the controller that will include the following:

- A description of the nature of the breach
- Categories of personal data affected
- Approximate number of data subjects affected

- Name and contact details of the Data Breach Response Team Consequences of the personal data breach
- Measures taken to address the personal data breach
- Any information relating to the data breach
- The Team will record the data breach

Personal data breach notification: Data controller to ICO

When the personal data breach or suspected data breach affects data that is being processed by the Council or Third Party as a data controller, the Team performs the following actions:

- To establish whether the personal data breach should be reported to the ICO.
- To establish the risk to the rights and freedoms of the data subject(s) affected. The team will conduct a Data Protection Impact Assessment on the processing activity connected to the data breach.
- If the personal data breach is not likely to result in a risk to the rights and freedoms of the affected data subject(s), no notification to the ICO is required. However, the data breach should be recorded in the Data Breach Register by the Information Rights Officer
- The ICO must be notified as soon as possible and wherever feasible within 72 hours, if the breach is likely to result in a risk to the rights and freedoms of the data subjects affected. Any possible reasons for delay beyond 72 hours must be communicated to the ICO.

The Information Rights Officer will send notifications to the ICO as approved by the DPO that will include the following:

- A description of the nature of the breach
- Categories of personal data affected
- Approximate number of data subjects affected
- Name and contact details of the Data Protection Officer
- Consequences of the personal data breach
- Measures taken to address the personal data breach
- Any information relating to the data breach

Personal data breach notification: Data controller to data subject

The Data Protection Officer must assess if the personal data breach is likely to result in high risk to the rights and freedoms of the data subject. If yes, the Data Protection Officer must notify as soon as possible the affected data subjects.

The notification to the data subjects must be clear and concise and must contain the information listed in the Appendix. Once you have drafted your notification to affected data subjects, wherever possible please contact the Team to review before the notifications are sent.

If, due to the number of affected data subjects, it is disproportionately difficult to notify each individual, the Team must take the necessary measures to ensure that the affected data subjects are notified by using appropriate, publicly available channels.

Accountability

Any individual who deliberately or maliciously breaches this Procedure may be subject to internal disciplinary action (up to and including termination of their employment); and may also face civil or criminal liability if their action violates the law. Inadvertent or accidental data breaches will also be investigated and further training provided if required.

Validity and document management

This document is valid as of 25th May 2018.The owner of this document is the Data Protection Team who must review and, if necessary, update the document at least once a year.

APPENDIX

DATA BREACH NOTIFICATION FORM TO DATA SUBJECTS

From: [Guildford Borough Council] To: [Affected data subject name and address] Sent by: • Post • Email
• Dear customer, we regret to inform you that on [date] we have discovered that we have been the subject of a personal data breach.
• As a result of the above mentioned personal data breach, the personal data concerning you might have been: • Disclosed • Destroyed • Lost • Modified • Accessed • Other [please specify other possible results]
• Please be aware that the personal data breach might have the following consequences: [list all possible consequences]
• The following measures have been taken/will be taken to address the data breach: [list all the measures taken]
If you have any questions or concerns regarding the data breach, we encourage you to contact [contact name], who is our Data Protection Officer, by email at DPO@guildford.gov.uk