DATA SECURITY BREACH MANAGEMENT POLICY AND PROCEDURES

Document history

Date	Version	Author	Changes made
18 September 2014	Version 1.0	Geraldine Sharman	None made by JSCG
8 August 2019	Version 2.0	Geraldine Sharman	Revised version
12 March 2020	Version 2.1	Sally Turnbull	Policy review
February 2022	Version 2.2	Sally Turnbull	Policy review
February 2023	Version 3	Sally Turnbull	*Revised version*

1. Introduction

1.1 Surrey Heath Borough Council (SHBC) is committed to ensuring that all personal data we process, including that of colleagues and customers, is managed appropriately and in compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018) (collectively referred to as "Data Protection legislation")

1.2 As SHBC processes personal data it is committed to ensuring all unauthorised or unlawful processing, loss, destruction of or damage to data (personal data breaches) are swiftly identified and reported within the Council and, where appropriate to the Information Commissioner's Office and affected individuals.

1.3 Human Resources may deal with negligent or malicious non-compliance with this policy through the disciplinary process.

1.4 Under the Data Protection Act 2018 and UK General Data Protection Regulation, Surrey Heath Borough Council is a Data Controller. This is a "person" who determines the purposes for which, and the manner in which, any personal data are, or, are not to be processed. The sixth Data Protection principle states that organisations, which process personal data, must ensure 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')."

1.5 As well as defining SHBC's policy, this procedure lays out the actions, once a breach has occurred.

2. Scope

2.1 This policy and procedure applies to all users of SHBC's information, data, information systems and the Council's physical buildings. It applies to not only staff and members but also where appropriate contractors, agency staff, service providers, consultants and anyone else engaged to work in the organisation and encompasses data, information, software, systems, and paper documents.

2.2 This policy should be read in conjunction with other relevant policies, including but not limited to:

- Data Protection Policy
- Information Security Policy
- Disciplinary Policy
- Social Media Policy
- Whistle-blowing Policy and Procedure

All staff, including all new starters, must read this policy as this forms part of the Staff Terms and Conditions.

2.3 Other useful documents:

- ICO Information Security Guide
- ICO Guidance on Personal Data Breaches
- EDPB Guidelines on Breach Management

3. Responsibilities

3.1 The **Senior Information Risk Owner (SIRO) (Strategic Director, Finance and Customer Services)** has overall responsibility for deciding whether to report personal data breaches to the ICO and/or to affected individuals but will delegate breach notification to the Data Protection Officer/Information Governance Manager. The Information Governance Manager and SIRO will meet on a regular basis to discuss Data Handling and Data Protection.

3.2 **Data Protection Officer(DPO) (Head of Legal Services)** has overall responsibility for monitoring compliance with this procedure. They will work, where necessary, with the Information Governance Manager, receiving and processing incident reports, assessing risk and advising the SIRO accordingly, and liaising with the ICO and the public as appropriate.

3.3 Although the Data Protection Officer has overall responsibility for monitoring compliance with this procedure, they will delegate the day-to day management of breaches to the **Information Governance Manager**, including receiving and processing incident reports and assessing the risk. In the absence of the Information Governance Manager, the Data Protection Officer will manage any breaches. The Information Governance Manager, will be the main contact with the Information Commissioner's Office.

3.4 **Executive Heads**, through Information Asset Owners, are responsible for ensuring that all staff are aware of their responsibilities to report incidents; for assisting the Data Protection Officer/Information Governance Manager in their duties through providing all appropriate information and support relevant to an incident; for continuing with appropriate incident management and mitigation.

3.5 **All staff** are responsible for immediately reporting any incident or breach affecting personal data held by the Council.

4. Types of breach

4.1 There are three key elements of information security that if compromised may result in a Personal Data Breach, these are identified as Confidentiality, Integrity and Availability (CIA)

4.1.1 Confidentiality breach – unauthorised or accidental disclosure of, or access to personal data

4.1.2 Availability breach – unauthorised or accidental loss of access to, or destruction of, personal data

4.1.3 Integrity breach – unauthorised or accidental alteration of personal data

4.2 A number of factors could cause data protection breaches. The following is a list of examples but it is not exhaustive and there may be others which will need to be considered at the time of the breach:

- loss or theft of data internally and externally to the Council
- loss or theft of equipment on which data is stored
- inappropriate sharing of access controls allowing unauthorised use, both electronic and paper
- equipment failure
- human error in dealing with personal information including sharing data, email insecurely, uploading in error
- unforeseen circumstances such as fire or flood
- hacking attack on the Council's ICT systems
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it
- unauthorised access into secure areas

5. Grading the personal data breach

Any incident must be graded according to the significance of the breach and the likelihood of those serious consequences occurring. The incident must be graded according to the impact on the individual or groups of individuals and not the organisations.

The significance is graded, rating the incident on a scale of 1-4. 1 being the lowest and 4 the highest

The likelihood of the consequences occurring are graded on a scale of 1-4. 1 being a non-occurrence and 4 indicating that it has occurred.

Where the personal data breach relates to a vulnerable group in society i.e. a child known to safeguarding or with mental health conditions or an adult with capacity issues or known to adult safeguarding, the minimum score will be a 2 in either significance or likelihood unless the incident has been contained. This will have the effect of automatically informing the Information Commissioner if one of the other axes scores above a 3.

Establish the likelihood that adverse effect has occurred

No	Likelihood	Description
1	Not occurred	There is absolute certainty that there can be no adverse effect.
2	Not likely to occur or incident involving vulnerable groups	There is no evidence that can prove that no adverse effect has occurred
3	Likely	It is likely that there will be an occurrence of an adverse effect arising from the breach
4	Occurred	There is a reported occurrence of an adverse effect arising from the breach

Grade the potential severity of the adverse effect on individuals

No	Effect	Description
1	No adverse effect	There is absolute certainty that no adverse effect can arise from the breach
2	Potentially some minor adverse effect or incident involving vulnerable groups	There is no absolute certainty that an effect can arise from the breach. This may be a loss of a name and address with no other confidential data lost.

3	Some adverse effect	An adverse effect may be the release of identifiable information into the public domain leading to some inconvenience or may delay a staff member being able to do their job
4	Major adverse effect/financial loss	There has been reported suffering arising from the breach or there has been some financial detriment occurred. The Councils is unable to provide key services

Both the severity of adverse effect and likelihood values form part of the breach assessment grid.

If the likelihood that an adverse effect has occurred is low the incident is not reportable to the ICO.

Breach Assessment Grid

The Council uses the below risk matrix tool to analyse the likelihood and severity of a risk giving an overall risk rating. Scores are determined by multiplying the 'likelihood' score with the 'severity' score which then gives and overall rating of low, medium or high risk. Any high risk must be reported to the ICO within 72 hours.

Severity

4 Major adverse effect	4 Low Risk	8 High Risk	12 High Risk	16 High Risk
3 Some adverse effect	3 Low Risk	6 Medium Risk	9 High Risk	12 High Risk
2 Potentially minor effect	2 Low Risk	4 Medium Risk	6 Medium Risk	8 High Risk
1 No adverse effect	1 Low Risk	2 Low Risk	3 Low Risk	4 Low Risk
	1 Not occurred	2 Not likely	3 Likely	4 Occurred

Likelihood

6. Notification of breaches once discovered

6.1 Instances of the loss of personal data are rare in the Council, however, the consequences to its reputation and the potential impacts on individuals of the loss of personal information means we need to take swift action in the event of a loss.

6.2 The person who discovers/receives a report of a breach must inform the Information Governance Manager and/or Data Protection Officer immediately. Notify any breach discovered outside of normal working hours as soon as is practicable during the next working day however any serious breaches that could cause serious adverse effect or media interest must be reported as a matter of urgency. The contact email address for data protection is data.protection@surreyheath.gov.uk

6.3 The Information Governance Manager and/or the Data Protection Officer, will then decide whether to involve other departments e.g. Human Resources, ICT.

7. Assessing the risks

7.1 The Information Governance Manager will carry out the initial assessment of the breach on the day it is reported and consider whether the event meets the UK GDPR definition of a personal data breach.

7.2 During this initial assessment, a risk assessment of the severity and likelihood of adverse effect on the rights and freedoms of the affected individual's, data subjects, will be undertaken this must be completed within 72 hours of the breach being reported.

7.3 This will consider the risks to the affected individuals arising from the personal data breach including adverse impact on their:

- Privacy
- Personal financial interests
- Other material damages
- Health and safety
- Emotional wellbeing

- Other non-material damages

7.4 In considering the risk, the Information Governance Manager will have support and advice from the Data Protection Officer and relevant Executive Head or Head of Service and other colleagues as required.

7.5 Factors to be considered (these factors are not exhaustive):

- The type of breach
- The nature, volume and sensitivity of the personal data breached
- How easy it is to identify individuals
- The potential consequences for individuals
- Any special characteristics of the data subject (for example they are children or otherwise venerable)

7.6 Some data security breaches will not lead to risks beyond the possible inconvenience to those who use the data to do their job, for example if a laptop is irreparably damaged or lost, or in line with the Information Security Policy, it is encrypted, and no data is stored on the device. There will be a monetary cost to the Council by the loss of the device but not a security breach.

7.7 Whilst these types of incidents can still have significant consequences, the risks are very different from those posed by, for example, the theft of customer data, whereby the data may be used to commit identity fraud.

7.8 Helpful tips for assessment of risks (these tips are not exhaustive):

- what type of data is involved?
- how sensitive is it? Is it sensitive personal details as defined by the Article 9 of UK GDPR (e.g. housing benefits) or other data types which are sensitive because of what might happen if it is misused (e.g. bank account details).
- if data has been lost or stolen, are there any protections in place such as encryption?
- what has happened to the data?

- can the data be restored or recreated?
- how usable is the lost data?
- if data has been stolen, could it be used for purposes which are harmful to the individuals to whom the data relates; if it has been damaged, this poses a different type and level of risk
- what could the data tell a third party about the individual? Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people
- how many individuals' personal data is affected by the breach? It is not necessarily the case that the bigger risks will accrue from the loss of large amounts of data but is certainly an important determining factor in the overall risk assessment
- who are the individuals whose data has been breached? Are they staff, customers, clients or suppliers?
- what harm can come to those individuals because of the breach? Are there risks to physical safety or reputation, financial loss, fraudulent use or a combination of these and other aspects of their life?
- are there wider consequences to consider such as a risk to loss of public confidence in one of the service areas?

8. Reporting personal data breaches to the affected individuals

8.1 As part of the risk assessment, consider whether the person/people whose information has been breached should be informed. Inform the person/people concerned, as suggested by guidance from the Information Commissioner unless to inform them will cause additional or undue distress/stress.

8.2 If the Information Governance Manager/Data Protection Officer considers the personal data breach a medium (orange) or high (red) risk, a report will be provided to the SIRO including a recommendation on whether to report the breach to the affected individuals.

8.3 If the SIRO decides to notify the individuals, consider the following:

- what is the most appropriate method of communication? Always bear in mind the security of the medium as well as the urgency of the situation
- the notification should include as a minimum, a description of how and when the breach occurred and what data was involved. Include details of what has already been done to respond to the risks posed by the breach
- give the individuals clear advice on what they should do to protect themselves and what the Council are willing to do on their behalf
- provide a means of contacting SHBC for further information. This could include a named individual, a helpline number, a web page or a combination of all of these.

9. Appointment of lead investigator

9.1 The Information Governance Manager will, in consultation with others, if necessary, decide who the Lead Investigator should be, who needs to be involved and will work with them to manage the breach. The Information Governance Manager is responsible for advising services on assessing the impact of any data breach of the Data Protection legislation. This can include recommendations to restore data security. The Information Governance Manager will appoint a lead investigator for serious breaches but could be appointed for minor breaches if the Information Governance Manager did not understand enough about the breach.

9.2 The Lead Investigator could be any of the following:

- a member of Audit and Investigations
- Executive Head

- Information Governance Officer
- Information Governance Manager
- a member of Human Resources
- a combination of the above

9.3 The Information Governance Manager will decide whom to notify.

9.4 The Senior Information Risk Owner (SIRO) will be notified of any minor breaches at the Information Governance Managers regular review meetings. For serious breaches (i.e. medium (orange) or high (red) risk), the SIRO must be informed immediately, the Chief Executive will also be made aware

9.5 The Lead Investigator/SIRO must also consider whether the police need to be informed. This could be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future. If credit card numbers are lost then tell the appropriate bankcard provider.

9.6 If necessary, consider notifying all staff to prevent additional breaches.

9.7 The Information Governance Manager will maintain a log with the details of **all** breaches. This will include who the Lead Investigator is, when the breach occurred, who is involved and what action must be taken after the breach.

10. Investigation procedure

10.1 The Information Governance Manager will begin investigation immediately on receipt of notification. They will complete urgently and wherever possible within 72 hours of the breach being discovered/reported a risk assessment to grade the breach; low (green), medium (orange) or high (red).

10.2 The Lead Investigator should ascertain whose data was involved in the breach, the person or people responsible for the breach, the potential

effect on the data subject and what further steps need to be taken to remedy the situation.

10.3 Breaches will require not just an initial investigation, risk assessment on the severity of the breach and containment of the situation but also a recovery plan including, where necessary damage limitation. This may often involve input from ICT, HR, Legal, Information Governance and the appropriate department. In some cases, contact with external stakeholders or suppliers may be required.

10.4 The Lead Investigator will establish the questions for interviews and then meet with the participants. This could be (but is not limited to or necessarily all of them) witnesses, victims and perpetrators, senior managers.

10.5 The Lead Investigator will identify if there is a need for expert advice from either professional advisers or Legal Services.

10.6 Issues to be addressed during the investigation will include:

- the date when the breach occurred
- the date when the breach was identified to SHBC and by whom
- the type of data and the number of records involved
- its sensitivity
- the circumstances of the release
- what protection is in place (for example encryption)
- what has happened to the data?
- whether the data could be put to any illegal or inappropriate use
- how many people are affected?
- what group of people has been affected (the public, suppliers etc)
- whether there are wider consequences of the breach

10.7 The Lead Investigator, via the Information Governance Manager, will keep an electronic record of all activities during the investigation. This could include the actions taken to mitigate the breach and lessons learnt. The reason for this is that the records may need sharing if there are actions by the police, Information Commissioner's Office, legal proceedings or Audit.

10.8 There could be a number of investigations going on at any one time for example by Human Resources and ICT.

10.9 The Information Governance Manager will assist the Lead Investigator, where necessary. This could include informing the Information Commissioner's Office of high risk incidents, calculating the severity of the incident, collating reports, implementing actions from the Information Governance report.

10.10 If systemic or on-going problems are identified, draw up an action plan to correct. If the breach warrants a disciplinary investigation (for example due to negligence), the Lead Investigator should pass on any relevant information to Human Resources who will make the final decision on sanctions against staff.

10.11 Where incident are risk assessed as medium (orange) or high (red) risk, the Lead Investigator should produce a report for the SIRO and be written with it in mind that it may be shared with the ICO.

10.12 The report must address the following:

- establish the facts (including those that may be disputed)
- include a chronology of events including the containment, recovery and how the breach has been investigated
- a risk analysis
- a commentary of the weight of evidence
- action to minimise/mitigate effect on individuals involved including whether the victims have been informed
- whether any other regulatory body and been informed and their response
- recommendations to reduce the chance of the same breach happening again

11. Containment

11.1 At the same time as an investigation is happening, containment and recovery must also happen.

11.2 The Lead Investigator must ascertain whether the breach is still occurring. If so, it must be stopped immediately and minimise the effect of the breach. This will involve liaison with appropriate staff. Examples might be the ICT Manager authorising the shutdown of a computer system or stopping the delivery of electronic mail.

11.3 Media and Marketing may need telling of a breach if there is a possibility of information published on the Internet or the press told and their assistance is required in managing a media response.

12. Reporting personal data breaches to the Information Commissioner's Office

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

12.2 The type of personal data breaches that must be reported to the ICO are if the breach is likely to result in a high 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 be on a case-by-case basis. There is no need to notify the ICO if there is not a risk to persons' rights and freedoms.

12.3 In the case of a personal data breach, the Council shall without undue delay and, where feasible, no later than 72 hours after becoming aware of a breach, notify the ICO, unless the personal data breach is unlikely to result in a high risk (red) to the rights and freedoms of an individual. A reason for the delay, if notification is not within 72 hours, is required along with the notification

12.4 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 Senior Information Risk Owner (SIRO). If the decision is to notify the ICO, the Information Governance Manager or if not available, the Data Protection Officer will act as liaison with the ICO.

12.5 When notifying the ICO the online reporting tool should be used, if not all information regarding the breach is available at the time of reporting this should not prevent the ICO being notified and instead the initial report should be submitted with the caveat that further information is to follow. Failing to notify the ICO of a breach when required to do so can result in a fine of up to €10 million.

12.6 The Data Protection Officer or Information Governance Manager in conjunction Human Resources will also need to consider whether any officer concerned with the breach will be subject to disciplinary procedures.

13. Review

13.1 A policy review will take place after a serious breach or after legislative changes, important changes in case law or guidance.

Report a breach - https://ico.org.uk/for-organisations/report-a-breach/