South Ribble Borough Council

Personal Data Incident & Data Breach Policy

Document Control

Document Title	Data Breach Policy
Version Number	1
Author	Kevin Conway
Approval date	
Review Date	12 months

1. Introduction

South Ribble Borough Council (the 'Council') collects, holds, processes, and shares personal data, a valuable asset that needs to be suitably protected.

Every care is taken to protect personal data from incidents (either accidentally or deliberately) to avoid a data protection breach that could compromise security.

Compromise of information, confidentiality, integrity, or availability may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative noncompliance, and/or financial costs.

2. Purpose and Scope of the Policy

The Council is obliged under Data Protection legislation [1] to have in place an institutional framework designed to ensure the security of all personal data during its lifecycle, including clear lines of responsibility.

This policy sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents across the Council.

This policy relates to all personal and special categories (sensitive) data held by the Council regardless of format.

This policy applies to;

- all part-time and full-time employees including those working from home or other remote/off-site locations
- elected Members
- all other workers including temporary, casual/agency staff, secondees and contractors, consultants, suppliers and data processors working for, or on behalf of the Council.
- any other person permitted to use South Ribble Borough Council's data resources and equipment.

The objective of this policy is to contain any breaches, to minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent further breaches

3. Responsibilities

- The **Chief Executive** has overall responsibility for ensuring our compliance with this policy and with Data Protection legislation;
- The **Deputy Chief Executive** as **Senior Information Risk Owner** (SIRO) has responsibility**,** at executive level, for oversight of data protection and other aspects of information governance. They also have overall decision making responsibilities as regards whether to report breaches to the Information Commissioners office (ICO)

[1] The General Data Protection Regulation (GDPR) and related EU and national legislation

- The **Senior Team Leader Customer Services and Data Protection** as **Data Protection Officer** (DPO) has day-to-day responsibility for monitoring compliance with this policy, advising the organisation on data protection matters and for receiving reports of personal data incidents for escalation as appropriate.
- **Directors and Assistant Directors** are responsible for ensuring that all systems, processes, records and datasets within their business area are compliant with this policy and with Data Protection legislation; for assisting the DPO in their duties through providing all appropriate information and support; for ensuring that their staff are aware of their data protection responsibilities; and consulting the DPO on new developments or issues affecting the use of personal data in the organisation; for ensuring Data Protection Impact Assessments are conducted as appropriate on data processing activities in their business area, drawing on advice from the DPO
- **All colleagues** are responsible for understanding and complying with relevant policies and procedures for handling personal data appropriate to their role, and for immediately reporting any event or breach affecting personal data held by the organisation.

4. Definitions / types of breach

For the purpose of this policy, data security breaches applies to Officers and Elected Members of the Council and includes both confirmed and suspected incidents.

An incident in the context of this policy is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to the Council's information assets and / or reputation

An incident includes but is not restricted to, the following:

- loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, tablet device, or paper record);
- equipment theft or failure;
- system failure;
- unauthorised use of, access to or modification of data or information systems;
- attempts (failed or successful) to gain unauthorised access to information or IT system(s);
- unauthorised disclosure of sensitive / confidential data;
- website defacement;
- hacking attack;
- unforeseen circumstances such as a fire or flood;
- human error;
- 'blagging' offences where information is obtained by deceiving the organisation holding it.

5. Reporting an incident

Any individual who accesses, uses or manages the Council's information is responsible for reporting data breach and information security incidents immediately to the Data Protection Officer/SIRO.

It could be that the notification of the breach is routed via the Council's Corporate Complaints process and this will be notified to the DPO automatically via the complaints process.

If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable.

The report must include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to people, the nature of the information, and how many individuals are involved. An Incident Report Form should be completed as part of the reporting process (refer to Appendix 1).

All staff should be aware that any deliberate breach of Data Protection legislation may result in the Council's Disciplinary Procedures being instigated.

6. Containment and recovery

The Data Protection Officer (DPO) will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach.

An initial assessment will be made by the DPO in liaison with relevant officer(s) to establish the severity of the breach and who will take the lead investigating the breach, as the Lead Investigation Officer (this will depend on the nature of the breach; in some cases it could be the DPO).

The Lead Investigation Officer (LIO) will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.

The LIO will establish who may need to be notified as part of the initial containment and will inform the police, where appropriate.

Advice from experts across the Council may be sought in resolving the incident promptly.

The LIO, in liaison with the relevant officer(s) will determine the suitable course of action to be taken to ensure a resolution to the incident.

7. Investigation and risk assessment

Post incident, an investigation will be undertaken by the DPO/LIO immediately and wherever possible, within 24 hours of the breach being discovered / reported.

If necessary a Data Protection Group is to be arranged comprising the SIRO, The Data Protection Officer and representatives from relevant departments such as Audit, Legal and HR. The purpose of the group is to discuss the incident and decide a course of action.

The investigation will need to take into account the following:

- the type of data involved;
- its sensitivity;
- the protections are in place (e.g. encryptions);
- what has happened to the data (e.g. has it been lost or stolen);
- whether the data could be put to any illegal or inappropriate use;
- data subject(s) affected by the breach, number of individuals involved and the potential effects on those data subject(s);
- whether there are wider consequences to the breach.

8. Notification

The LIO and/or the DPO, in consultation with the Data Protection Officers Group will establish whether the Information Commissioner's Office will need to be notified of the breach, and if so, notify them within 72 hours of becoming aware of the breach, where feasible.

Every incident should be assessed on a case by case basis; however, the following will need to be considered:

- whether the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms under Data Protection legislation[2];
- whether notification would assist the individual(s) affected (e.g. could they act on the information to mitigate risks?);
- whether notification would help prevent the unauthorised or unlawful use of personal data;
- whether there are any legal / contractual notification requirements;
- the dangers of over notifying. Not every incident warrants notification and over notification may cause disproportionate enquiries and work.

Individuals whose personal data has been affected by the incident, and where it has been considered likely to result in a high risk of adversely affecting that individual's rights and freedoms, will be informed without undue delay. Notification will include a description of how and when the breach occurred and the data involved. Specific and clear advice will be given on what they can do to protect themselves, and include what action has already been taken to mitigate the risks. Individuals will also be provided with a way in which they can contact the Council for further information or to ask questions on what has occurred.

[2] Individual Rights: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individualrights/

The LIO and/or the DPO must consider notifying third parties such as the police, insurers, banks or credit card companies, and trade unions. This would 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.

The LIO and / or the DPO will consider whether the Communications Team should be informed regarding a press release and to be ready to handle any incoming press enquiries.

A record will be kept of any personal data breach, regardless of whether notification was required (Data Breach Database)

9. Evaluation and response

Once the initial incident is contained, the DPO will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.

Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

The review will consider:

- where and how personal data is held and where and how it is stored;
- where the biggest risks lie including identifying potential weak points within existing security measures;
- whether methods of transmission are secure; sharing minimum amount of data necessary;
- staff awareness;
- implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security

9.1. If necessary, a report recommending any changes to systems, policies and procedures will be considered by the Leadership Team

10. Policy Review

This policy will be updated as necessary and reviewed as a minimum on a 12 month basis to reflect best practice and to ensure compliance with any changes or amendments to relevant legislation

Data Breach Report Form

Please act promptly to report any data breaches. If you discover a data breach, please notify your Head of Service immediately, complete Section 1 of this form and return it to the Data Protection Officer (info@southribble.gov.uk) and IT Helpdesk (ithelpdesk@southribble.gov.uk) where appropriate.

Section 1: **Notification of Security Breach**	**To be completed by Head of Service / person reporting incident**
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Contact details of person reporting incident:	
Brief description of incident or details of the information lost:	
Number of Data Subjects affected, if known:	
Has any personal data been placed at risk? If so, please provide details:	
Brief description of any action taken at the time of discovery:	
For use by the Data Protection Officer	
Received by	
On (date):	
Forwarded for action to:	
On (Date):	

Section 1: **Assessment of Severity**	**To be completed by the LIO/DPO in consultation with the Head of Service affected by the breach and if appropriate IT where applicable.**
Details of the IT systems, equipment, devices, records involved in the security breach	
Details of Information Loss	
What is the nature of the information lost?	
How much data has been lost?	
Is the information unique? Will its loss have adverse operational, financial, legal, liability or reputational consequences for the Council or third parties?	
How many data subjects are affected?	
Is the data bound by any contractual security arrangements?	
What is the nature of the sensitivity of the data? Please provide details of any types of information that fall into any of the following categories>	
HIGH RISK personal data **Special categories personal data** (as defined in Data Protection Legislation) relating to a natural person's a) health b) racial or ethnic origin; c) sex life or sexual orientation; d) political opinions ; e) religious beliefs; f) trade union membership; g) genetic information; h) biometrics (where used for ID purposes);	
Information that could be used to commit identity fraud such as; personal bank account and other financial information; national identifiers, such as National Insurance Number and copies of passports and visas;	
Personal information relating to vulnerable adults and children;	
Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed;	
Security information that would compromise the safety of individuals if disclosed.	
Data Protection Officer and/or Lead Investigation Officer to consider whether it should be escalated to the Extended Leadership Team.	

Section 2: **Action Taken**	**To be completed by Data Protection Office and/or Lead Investigation Officer**
Incident Number	e.g. year/001
Report Received by:	
On (Date):	
Action taken by responsible officer/s:	
Was incident reported to police	**YES / NO** If YES, notified on (Date): Details:
Follow up action required / recommended:	
Reported to Data Protection Officer and Lead Officer on (date):	
Reported to other internal stakeholders (details, dates):	
For use by the Data Protection Officer and/or Lead Investigation Officer	
Notification to ICO	**YES / NO** If YES, notified on (Date): Details:
Notification to Data Subjects	**YES / NO** If YES, notified on (Date): Details:
Notification to other external, regulator/stakeholder	**YES / NO** If YES, notified on (Date): Details:
On (Date):	