SALISBURY CITY COUNCIL

Data Security Breach Incident Policy

Policy Number	Version	Owner	Doc No.	PDF No.	Date Published	Review Due	Review Team
CS044	1	CSM	65292	77102	13 Jan ‘20	Jan ‘22	Man

Distribution

Internal: All SCC Staff

External: Website/Councillors/Partners

1. What is Personal Data?

1.1. Personal data relates to a living person who can be identified from that data.
1.2. Identification can be by the information alone or in conjunction with other information in the data controller's possession or likely to come into.
1.3. The processing of personal data is governed by the General Data Protection Regulation (the "GDPR").

2. What is the Data Controller?

2.1. The Data Controller decides how your personal data is processed and for what purposes. The Data Controller for Salisbury City Council is the Corporate Services Manager.

3. How do we process your personal data?

3.1. Salisbury City Council complies with its obligations under the "GDPR" by keeping personal data up to date; by storing and destroying it securely; by not collecting or retaining excessive amounts of data; by protecting personal data from loss, misuse, unauthorised access and disclosure and by ensuring that appropriate technical measures are in place to protect personal data.
3.2. We use your personal data for the following purposes: -
  3.2.1. To provide our services; inform you of news; events, activities and services that will be occurring in which you may be interested
  3.2.2. To manage our employees and volunteers
  3.2.3. To maintain our own accounts and records
  3.2.4. To administer our records

4. Will you share my personal data?

4.1. SCC will not disclose or share your information to a third party without consent
4.2. SCC will seek your consent before any new processing of information
4.3. **Data Sharing Consent Form (DOC 76562)** shown at **Appendix A**

5. What is the legal basis for processing personal data?

5.1. Processing is necessary for carrying out obligations under employment
5.2. Processing is carried out for customers, suppliers, user groups or those who have regular contact with the council

6. Your rights and your personal data

6.1. Unless subject to an exemption under the GDPR, you have the following rights with respect to your personal data:
  6.1.1. The right to request a copy of your personal data which SCC holds about you
  6.1.2. The right to request that SCC corrects any personal data if it is found to be inaccurate or out of date

6.1.3. The right to request your personal data is erased where it is no longer necessary for SCC to retain such data
6.1.4. The right to withdraw your consent to the processing at any time
6.1.5. The right to request that the data controller provide the data subject with his/her personal data
6.1.6. The right, where there is a dispute in relation to the accuracy or processing of your personal data, to request a restriction is placed on further processing
6.1.7. The right to object to the processing of personal data
6.1.8. The right to lodge a complaint with the Information Commissioners Office.

7. What is a Data Security Breach?

7.1. Data security breaches are common occurrences whether caused through human error or malicious intent. As technology changes and the creation of data and information grows, there are more ways by which data can be breached.
7.2. The council needs to have in place a robust and systematic process for responding to any reported data security breach, to ensure it can act lawfully and protect its information.
7.3. This policy applies to all council information, regardless of format, and is applicable to all staff, elected members, visitors and contractors.
7.4. Data security breaches include both confirmed and suspected incidents.

8. Aims of this policy

8.1. The aim of this policy is to standardise the council's response to any reported data breach incident and ensure that they are appropriately logged.
8.2. A standardised approach to all reported incidents aims to ensure that:
8.2.1. incidents are properly investigated
8.2.2. incidents are handled by authorised personnel
8.2.3. incidents are recorded and documented
8.2.4. the impact of the incidents are understood and action is taken to prevent further damage
8.2.5. evidence is recorded in a form that will withstand internal and external scrutiny
8.2.6. external bodies or data subjects are informed as required
8.2.7. the incidents are dealt with in a timely manner and normal operations restored
8.2.8. the incidents are reviewed to identify improvements

9. Definition

9.1. A data security breach is considered to be "any loss of, or unauthorised access to, council data".
9.2. Examples of data security breaches may include:
9.2.1. Loss or theft of data or equipment on which data is stored
9.2.2. Unauthorised access to confidential or highly confidential Data
9.2.3. Equipment failure

9.2.4. Human error
9.2.5. Unforeseen circumstances such as a fire or flood
9.2.6. Hacking attack

10. Responsibilities

10.1. All information users are responsible for reporting actual, suspected, threatened or potential information security incidents and for assisting with investigations as required, particularly if urgent action must be taken to prevent further damage.
10.2. Managers are responsible for ensuring that staff in their area act in compliance with this policy and assist with investigations as required.
10.3. Lead responsible officers will oversee the management of the breach in accordance with the **Data Breach Management Plan**. See **Appendix B**
10.4. Data security breaches will vary in impact and risk depending on the content and the quantity of the data involved, therefore it is important that the council is able to quickly identify the classification of the data and respond to all reported incidents in a timely and thorough manner.
10.5. All reported incidents will need to include the appropriate data classification in order for assessment of risk to be conducted.
10.6. Data classification referred to in this policy means:
10.6.1. **Public Data**: Information intended for public use, or information which can be made public without any negative impact for the council.
10.6.2. **Internal Data**: Information regarding the day-to-day business and operations of the council. Primarily for staff and elected member use, though some information may be useful to third parties who work with the council.
10.6.3. **Confidential Data**: Information of a more sensitive nature for the business and operations of the council, representing the intellectual property.
10.6.4. **Highly confidential Data**: Information that, if released, will cause significant damage to the council's business activities or reputation, or would lead to breach of the Data Protection Act. Access to this information should be highly restricted.

11. Data Security Breach Reporting

11.1. Confirmed or suspected data security breaches should be reported promptly to the Corporate Services Manager.
11.2. The report should include full and accurate details of the incident including who is reporting the incident and what classification of data is involved.
11.3. The **Data Breach Incident Report** form should be completed as part of the reporting process. See **Appendix C (DOC 76561)**.
11.4. Once a data breach has been reported an initial assessment will be made to establish the severity of the breach using the **Data Breach Incident – Evaluation of Severity**. See **Appendix D (DOC 65684)**
11.5. All data security breaches will be logged on the Incident Log to ensure appropriate oversight in the types and frequency of confirmed incidents for management and reporting purposes.

12. Data Breach Management Plan

12.1. The management response to any reported data security breach will involve the following four elements.

12.1.1. Containment and Recovery
12.1.2. Assessment of Risks
12.1.3. Consideration of Further Notification
12.1.4. Evaluation and Response

Council Staff, elected members, contractors and visitors who act in breach of this policy, or who do not act to implement it, may be subject to disciplinary procedures or other appropriate sanctions.

You can contact the Information Commissioners Office at:
The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire. SK9 5AF
☎ 0303 123 1113
https://ico.org.uk/global/contact-us/email/

Appendix A.

Data Sharing Consent Form

Your privacy is important to us, and we want to communicate with residents in a way which has their consent, and which is in line with UK law on data protection. As a result of a change in UK law, we now need your consent to how we contact you.

Please fill in the contact details you want us to use to communicate with you:

Name:
Address:

Email Address:
Phone Number:

By signing this form you are confirming that you are consenting to the Salisbury City Council holding and processing your personal data for the following purposes (please tick the boxes where you grant consent):

I consent to the council contacting me by ☐ post ☐ phone or ☐email.

☐ To keep me informed about news, events, activities and services

☐ To share my contact details with colleagues within Salisbury City Council so they can keep me informed about news, events, activities and services

☐ To share my contact details with third parties so they can keep me informed about news, events, activities and services related to Salisbury City Council

Signed: Dated:

You can grant consent to all the purposes; one of the purposes or none of the purposes. Where you do not grant consent we will not be able to use your personal data; (so for example we may not be able to let you know about forthcoming services and events); except in certain limited situations, such as where required to do so by law or to protect members of the public from serious harm.

Find out more about how we use your data from our “Privacy Notice” which is available on our website.

You can withdraw or change your consent at any time by contacting
info@salisburycitycouncil.gov.uk or ☎ 01722 342860

Appendix B

Data Breach Management Plan

This guidance sets out what to consider in the event of a security breach

Step One – Containment and Recovery

1. What type of data is involved, where and how it is stored? (Dealing with a data security breach is much easier if you know what data are involved)
2. What harm can come to the individuals involved? (Are there risks to physical safety or reputation, or of financial loss?)

If appropriate, inform the police

Step Two - Assessing the Risks

1. Who needs to be made aware of the breach?
2. Inform them of what they are expected to do. (This could be isolating or closing down a section of the IT network, finding a lost piece of equipment or simply changing the codes of an access door).
3. Is there anything you can do to recover any losses and limit the damage the breach can cause? (Physical recovery of equipment, the use of back up tapes to restore lost or damaged data or ensuring that staff recognise when someone tries to use stolen data to access accounts).
4. Are there wider consequences to consider such as a risk to reputation or loss of public confidence?
5. How sensitive is it? (Salary records or bank account details)
6. Are there any protections in place such as encryption?
7. Could the data be used for purposes which are harmful to the individuals to whom the data relates?
8. How many individuals' personal data are affected and who are they? (Whether they are staff, customers, clients or suppliers will determine the level of risk)
9. If bank details are lost contact the bank for advice to prevent fraudulent use
10. What could the data tell a third party about the individual? (Trivial snippets of information could help a fraudster build up a detailed picture of other people)

Step Three – Notifications of a breach

1. Are there any legal or contractual requirements? (You might need to notify third parties such as the police, insurers, bank or credit card companies or trade unions)
2. The ICO should only be notified when the breach involves personal data.
3. Consider how notification can be age appropriate? (Children or vulnerable adults)
4. Can notification help the individual? (Cancelling a credit card or password).
5. Consider 'over notifying'. (Notifying a whole customer database may cause disproportionate enquiries and work)
7. Notification should include a description of how and when the breach occurred and what data was involved. (Include details of what you have already done)
8. Provide a contact name and number.

Step Four – Evaluation and Response

1. Monitor staff awareness of security issues and fill gaps through training
2. Establish where the biggest risks lie. (Is personal data held in one location?)
3. Risks will arise when sharing with or disclosing to others. (Make sure the method of transmission is secure and only share or disclose the minimum data necessary).
4. Identify weak points (Portable devices or public access points)
5. Consider establishing a staff group to discuss ‘what if’ scenarios (To highlight risks and weaknesses and give staff at the opportunity to suggest solutions)
6. Consider including a data security breach section in the Business Continuity Plan

Appendix C

Data Breach Incident Report Form

Please act promptly to report any data breaches.
If you discover a data breach, please notify your Line Manager/ Corporate Service Manager immediately

	Report prepared by: **Date:** **On behalf of:**	**Name:** **Date:** **Organisation:**
1.	**Description of the Data Breach:**	*Nature of breach e.g. theft/disclosed in error/technical problems:*
2.	**Time and Date breach was identified and by whom:**	
3.	**Contact details: Telephone/Email**	
4.	**Type and quantity of personal data:**	*Title or name of the document/s; What personal information is included – Name; Address; DoB; Bank account details; description of information about an individual (health issues; case hearing/decisions etc.)*
5.	**Classification of data breached** **(In accordance with SCC Data Security Breach Incident Policy)**	*i. Public Data* *ii. Internal Data* *iii. Confidential Data* *iv. Highly Confidential Data*
6.	**Breach of procedure/policy by staff member:**	*Has there been a breach of policy?* *Has appropriate action been taken?* *Internal/external staff?*

7.	**Is the breach contained or ongoing:**	
8.	**If ongoing what actions are being taken to recover the data:**	
9.	**Who has been informed of the breach?**	
10.	**Has a subject access request been received:**	***Has the data subject been notified? If not, explain why not?*** ***What advice has been given to affected data subjects?***
11.	**Procedure changes to reduce risks of future data loss:**	
12.	**Any other relevant information:**	

Email form to Corporate Services Manager:
jwhitty@salisburycitycouncil.gov.uk

	Received by:	
	Date/Time	

Appendix D

Data Breach Incident - Evaluation of Severity

Assessment of incident severity would be made by the Corporate Services Officer upon the following criteria:

High Criticality: Major Incident	***Contact:***
• **Highly Confidential/Confidential Data** • **Personal data breach involves > 1000 individuals** • **External third party data involved** • **Significant or irreversible consequences** • **Likely media coverage** • **Immediate response required regardless of whether it is contained or not** • **Require significant response beyond normal operating procedures**	**Lead Responsible Officer:** • **Corporate Services Manager** **Other relevant contacts:** • **City Clerk** • **Contact external parties i.e. Police/individuals impacted/ Information Commissioner's Office**
Moderate Criticality: Serious Incident	**Contact:**
• **Confidential Data** • **Not contained within Salisbury City Council** • **Breach involves personal data of more than 100 people** • **Significant inconvenience will be experienced by individuals impacted** • **Incident may not be contained** • **Incident does not require immediate response** • **Incident response may require notification to Council's senior managers**	**Lead Responsible Officer:** • **Corporate Services Manager** **Other relevant contacts:** • **City Clerk**
Low Criticality: Minor Incident	**Contact:**
• **Internal or Confidential data** • **Small number of individual involved** • **Risk to Council low** • **Inconvenience may be suffered by individuals impacted** • **Incident can be responded to during working hours** **Example:** **Email sent to wrong recipient** **Loss of encrypted mobile device**	**Lead Responsible Officer:** • **Corporate Services Manager** **Other relevant contacts:** • **Line Manager** • **All Management**