CREDITON
TOWN COUNCIL

Manor Office
6 North Street
Crediton
Devon
EX17 2BR
Telephone: 01363 773717
Email: reception@crediton.gov.uk

Data Breach Policy

Introduction

Crediton Town Council (CTC) issues this policy to meet the requirements of the General Data Protection Regulations (GDPR) 2018 for the handling of personal data in its role as a Data Controller.

This policy applies to councillors and all employees of CTC including contract, agency and temporary staff, volunteers and employees of partner organisations working for CTC.

CTC must have in place a robust and systematic process for responding to any reported issues, to ensure it can act responsibly and protect personal data which it holds. In any situation where staff are uncertain whether an incident constitutes a breach of security, it must be reported to a line manager. Appropriate measures will be implemented to protect personal data from incidents (either deliberate or accidental), to avoid issues that could compromise security.

Data Breaches

A Data Breach is defined as the compromising of the confidentiality, integrity, or availability of personal data which may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative non-compliance, and/or financial costs.

A Data Breach can come in many forms, but the most common are as follows:

- Inappropriate sharing or dissemination
- Hacking, malware, data corruption
- Unescorted visitors accessing data
- Non-secure disposal of data
- Loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, iPad/tablet device, paper record)
- 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 (e.g. login details, emails to the wrong recipient, not using BCC, post to the wrong address)
- Website defacement
- Unforeseen circumstances such as a fire or flood
- Breaches of policy such as filing cabinets left unlocked

Near misses can include, but are not limited to, scenarios such as emails sent to the wrong recipient where a non-delivery report bounces back. The aim of this policy is to standardise the CTC's response to any Data Breach and ensure that they are appropriately logged and managed in accordance with the law and best practice, so that:

- Incidents are reported swiftly and can be properly investigated
- Incidents are dealt with in a timely manner and normal operations restored
- Incidents are recorded and documented
- The impact of the incident is understood, and action is taken to prevent further damage
- The Data Protection Officer (DPO) and the Information Commissioner's Office (ICO) and data subjects are informed as required in more serious cases.
- Incidents are reviewed and lessons learned.

This procedure sets out how CTC will manage a report of a suspected data breach. The aim is to ensure that where data is misdirected, lost, hacked or stolen, inappropriately accessed or damaged, the incident is properly investigated and reported and any necessary action is taken to rectify the situation. The form at Appendix A will be used when reporting a suspected data breach.

If there are IT issues, such as the security of the network being compromised, the Town Clerk should be informed immediately.
The GDPR applies to both Data Controllers (CTC itself) and to Data Handlers. Therefore, 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.

The Town Clerk is responsible for ensuring that staff in their area act in compliance with this policy and assist with investigations as required. The Town Clerk, acting as the Data Protection Officer (DPO), will be responsible for overseeing management of the breach in accordance with the Policy. Suitable further delegation may be appropriate in some circumstances.

Security Impact Management (SIM)
CTC's DPO shall complete the following phases of SIM:

1. Preparation – CTC will understand its environment and be able to access the necessary resources in times of incidents. It will also ensure its staff are aware of how to identify and report breaches.
2. Identification – CTC will determine whether there has been a breach, or a near miss, it will also assess the scope of the breach, and the sensitivity on a risk basis.
3. Containment and Eradication – CTC will take immediate appropriate steps to minimise the effect of the breach. It will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause and will establish who may need to be notified as part of the initial containment and will inform the police and other enforcement bodies where appropriate.
4. Recovery – CTC will determine the suitable course of action to be taken to ensure a resolution to the incident. This may include re-establishing systems to normal operations, possibly via reinstall or restore from backup.
5. Learning from Experience (LfE) – an assessment will be made on the likely distress on any affected data subjects. This will then form the decision on whether to report this to the regulator (ICO) which must be reported within 72 hours, and to the affected data subjects which must be done without undue delay. Officers may also be notified to handle any queries and release statements.

Phases (2) to (5) will form part of the investigation process. This process should commence immediately and wherever possible within 24 hours of the breach being discovered or reported. If necessary, a report recommending any changes to systems, policies and procedures will be considered by the Town Clerk. This will include the decision on whether to report to the regulator and affected data subjects. A review of existing controls will be undertaken to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring. The review will consider:

- Whether policy controls are sufficient
- Whether training and awareness can be amended and/or improved
- Where and how personal data is held and where and how it is stored
- Where the biggest risks are apparent and any additional mitigations
- Whether methods of transmission are secure
- Whether any data sharing is necessary.

Monitoring and Compliance

Compliance with this policy shall be monitored through a review process. This will be agreed with the Data Protection Officer, and compliance will be reported to line management. Should it be found that this policy has not been complied with, or if an intentional breach of the policy has taken place, the organisation shall have full authority to take the immediate steps considered necessary, including disciplinary action.

This policy will be reviewed upon any change of Data Protection Officer or change of legislation and no less than every two years.

Appendix A

Data Incident Reporting Form

Name of person completing the form:
Contact details:

1. About the Incident	
Date and time of incident	
Location of incident	
Date and time of notification incident occurred (providing explanations if there was any delay in reporting the incident)	
Name of person who notified the Council that the incident took place.	
Description of incident	

2. Recovery of the Data	
Measures taken to contain the incident (including limiting the initial damage, notifying the Police of theft, providing support to affected data subjects etc)	
Details of attempts to recover data (including dates and times)	