Data Breach Policy

1. Introduction

Trowbridge Town Council 'The Council' 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 Trowbridge Town Council including contract, agency and temporary staff, volunteers and employees of partner organisations working for Trowbridge Town Council.

The Council 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 the Customer Service Manager. Appropriate measures will be implemented to protect personal data from incidents (either deliberate or accidental), to avoid issues that could compromise security.

2. 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, USB stick, iPad/tablet device, paper record, or access badge).*
- 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
    - Server Room door left open
    - Filing cabinets left unlocked
    - Temporary loss/misplacement of confidential or sensitive data or equipment on which such data is stored *(e.g. loss of laptop, USB stick, iPad/tablet device, paper record, or access badge).*

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 Council'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 the Council 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.

If there are IT issues, such as the security of the network being compromised, the Facilities Manager, should be informed immediately.

The GDPR applies to both Data Controllers (the Council 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.

Heads of Service are responsible for ensuring that staff in their area act in compliance with this policy and assist with investigations as required. The Customer Service Manager, and the Council's 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.

3. Reporting a Breach

The quick response to a suspected or actual data breach is key. All those in the scope of this policy have a responsibility to report a suspected or actual data breach. If this is discovered or occurs out of hours, then this should be reported as soon as practically possible. This should be done through the completion of the reporting form (Appendix 1) which should be then sent to Customer Service Manager at aby.cooper@trowbridge.gov.uk who will liaise with the Data Protection Officer.

4. Security Incident Management (SIM)

Trowbridge Town Council's lead officer shall complete the following phases of SIM (which are detailed in Appendix 2) with advice from its Data Protection Officer:

a) **Preparation** – The Council 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.
b) **Identification** – The Council 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.
c) **Containment & Eradication** – The Council 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.
d) **Recovery** – The Council 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.
e) **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. The Council's Communications/Press Team may also be notified to handle any queries and release statements.

Phases (b) to (e) 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

5. 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 the Heads of Services. 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.

Review this Policy upon;

- **Change of Data Protection Officer**
- **Change of Legislation**

Policy approved on 7/7/2020

Appendix 1 – Data Incident Reporting Form

1. About the incident	
Date and time of incident	
Where did the incident occur?	
Date (and time where possible) of notification to the organisation	*If there was any delay in reporting the incident, please explain why this was*
Who notified us of the incident?	
Describe the incident in as much detail as possible, including dates, what happened, when, how and why?	*Include names of staff and data subject(s). Identifying information will be anonymised for any reporting purposes*
2. Recovery of the data	
What have you done to contain the incident?	*e.g. limiting the initial damage, notifying the police of theft, providing support to affected data subjects*
Please provide details of how you have recovered or attempted to recover the data, and when	*Consider collecting the lost data, rather than relying on an unintended recipient to dispose of it*
3. About the affected people (the data subjects)	
How many individuals' data has been disclosed?	
Are the affected individuals aware of the incident, and if so, what was their reaction?	
When and how were they made aware/informed?	
Have any of the affected individuals made a complaint about the incident?	
Are there any potential consequences and/or adverse effects on the individuals? What steps have been taken/planned to mitigate the effect?	
Your name and contact details:	

Appendix 2 - Security Incident Management (SIM): Record of Work

This document provides the documented evidence and audit trail of a reported information security incident. It is designed to operate alongside the Council's Data Protection Policy, and Data Breach Policy.

This form is to be completed by the Customer Service Manager in the organisation.

The incident may require additional input and support from the organisation's Data Protection Officer, ICT, and potentially other specialist bodies (e.g. National Cyber Security Centre – NCSC)

Incident No:	
Severity (H, M, L):	
Basis for initial severity rating:	
Incident Handler(s):	
Date reported to organisation:	
By whom:	
Date reported to Incident handler:	
By whom:	
Date incident occurred:	
Senior Management notified (date):	

Summary of breach:	

Incident Response Phase	Evidence/Actions Taken
1. Preparation Gather and learn the necessary tools, become familiar with your environment	• IT Support provided by (INSERT) • DPO provided by i-West • The Record of Processing Activities (RoPA) will provide details of data, flows, owners, custodians, and third parties – link to the RoPA • GDPR training rolled out to staff
2. Identification Detect the incident – is it an incident (breach of policy), a near miss, or a data breach? Determine its scope, and involve the appropriate parties	
3. Containment Contain the incident to minimize its effect on other IT resources	
4. Eradication Eliminate the affected elements e.g. remove the malware and scan for anything remaining	

5. Recovery Restore the system to normal operations, possibly via reinstall or backup.	
6. Wrap U Document the lessons learned and actions to reduce the risk of the incident/breach/near miss re-occurring Document the decision to report to both the affected data subjects and the ICO.	*If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay* **Decision to report to data subjects** - Yes/No Based on: Officer: Signed: Date:
	Establish the likelihood and severity of the resulting risk to people's rights and freedoms - A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned **Decision to report to ICO** - Yes/No Based on: Officer: Signed: Date:

Signature……..Dated…….