Broseley Town Council

DATA BREACH POLICY

What is a data breach?

A personal data breach is the accidental or unlawful destruction, loss, theft, alteration, unauthorised disclosure of, or access to, personal data.

Examples include:

- Access by an unauthorised third party.
- Deliberate or accidental action (or inaction) by a data controller or data processor.
- Personal data being sent to an incorrect recipient.
- Computing devices containing personal data being lost or stolen.
- Alteration of personal data without permission.
- Loss of availability of personal data.

Data protection

As a data processor the Town Council has a duty to comply with the Data Protection Act 2018. In order to ensure that there are no data breaches the Town Council operates in accordance with its Password Policy and all computers are password protected. Hard copies of personal data are stored safely in locked containers and access is strictly controlled.

Consequences of a personal data breach

A data breach can have a detrimental effect on individuals and can lead to a loss of control of personal data, discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality, damage to property or social disadvantage.

Risk assessing data breaches

When a security incident occurs, the Council will quickly establish whether a personal data breach has taken place and, if so, will promptly take steps to address it, including informing the ICO if required. Upon becoming aware of a breach, the Council will contain it and assess the potential adverse consequences for individuals, dependent upon how serious or substantial these are, and how likely they are to happen.

The Council will investigate whether or not the breach was a result of human error or a systemic issue and see how a recurrence can be prevented.

Informing individuals about a breach

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the Council will inform those concerned directly as soon as possible.

A 'high risk' means that the individual(s) concerned must be informed of a data breach before the ICO is informed so that individuals can take steps to protect themselves from the effect of a breach. The Council will still contact the ICO if it is deemed that the individual does not need to be informed.

The Town Council's duty to report a data breach

If it meets the threshold for reporting a personal data breach, a breach must be reported to the ICO without undue delay and within 72 hours. All the facts must be put together and the time starts from when the breach is discovered and not when it actually happened.

Breaches should be reported to the breach reporting team on 0303 123 1113 or https://ico.org.uk/pdb

The Council will make every attempt to contain the breach and recover the data and protect those who are impacted.

What information the Council must provide to Individuals when informing them about a data breach

When a data breach occurs, the following information must be provided to those affected:

1. A description of the nature of the personal data breach.
2. The name and contact details of any data protection officer the Council has, or another point of contact where more information can be obtained.
3. A description of the likely consequences of the personal data breach.
4. A description of the measures the Council has taken or proposes to take to deal with the personal data breach and, where appropriate, a description of the measures taken by the Council to mitigate any possible adverse effects.

If possible, the Council will provide specific and clear advice to individuals on the steps they can take to protect themselves, and what the Council is willing to do to assist them. This may include:

- Forcing a password reset.
- Advising individuals to use strong, unique passwords.
- Telling them to guard against phishing emails or fraudulent activity on their accounts.

What information should be reported to the ICO

When a data breach occurs, the following information must be reported to the ICO:

1. Details about what happened.
2. How it happened.
3. How it was discovered
4. What preventative measure are in place.
5. Whether the breach was caused by a cyber incident.
6. The time and date when the breach happened.
7. The time and date when the breach was discovered.
8. The type of personal data included in the breach.
9. The number of personal data records concerned.
10. The number of data subjects that could be affected and the categories of the data subjects affected.
11. Potential consequences of the breach.
12. Whether the data breach is likely to result in a high risk to the data subjects.
13. Whether the person involved in the breach has received data protection training in the last two years.
14. The action taken by the Town Council, or what action will be taken as a result of the breach.
15. Whether action has been taken to contain the breach with a description of remedial actions.
16. Steps that the Town Council will take to prevent a recurrence and when it is expected to be completed.
17. Whether the data subjects have been informed about the breach.
18. Whether any other organisations will be informed about the breach.
19. Details about the Town Council and the person making the report.

This information may be recorded using an online form and sent to icocasework@ico.org.uk

Action to contain a data breach

If information has been sent to someone by mistake, they will be asked to delete/destroy it, send it back securely or have it ready to be collected.

If the breach is due to a stolen computer, the data will be wiped remotely if possible. This will help to minimise the risk of personal data falling into the wrong hands. All passwords will be changed to avoid/contain a cyber incident. If unsure what to do the Council will contact the ICO for advice.

Action to protect those affected

The Council will assess the risk of harm to those affected. Unless there is a high risk to individuals affected by a data breach they will not be notified. Where it will lead to a risk of harm or detriment, those affected will be notified and advised about any action they can take to protect themselves and how the Council can help them.

Recording data breaches

The Council will maintain a record of all data breaches whether or not they need to be reported to the ICO. The record will document:

- The facts regarding the breach.
- Its effects.
- The remedial action taken.

This policy has been developed from information provided by the ICO and is available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/#riskassessingdata

Adopted:	*February 2021*
Minute no:	*512(c)*
Version:	*1*
Next review date:	*January 2023*