BINGLEY TOWN COUNCIL

Bingley Town Council, Myrtle Place, Bingley, BD16 2LF

Security Incident Policy

Date of review: 31st October 2023
Next review date: October 2024

What is a breach?
A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Policy
This policy specifies the actions with respect to breaches of personal data.
Examples - personal data breaches can include:

- Access by an unauthorised third party;
- Deliberate or accidental action (or inaction) by a controller or processor;
- Sending personal data 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.

Dealing with an incident

Reporting Point
On discovery of an incident either as a result of automatic notification, accidental discovery, manual record checking or any other means, all personnel shall;
1. Report the incident to the reporting points:
- The Town Clerk and the Chair of the Town Council:
email: townclerk@bingleytowncouncil.gov.uk.
email: philippa.gibbons@bingleytowncouncil.
2. The email report should be followed by a telephone call to the Town Clerk or Chair.
3. Should neither the Town Clerk nor the Chair be available, the Vice-Chair of the Council should be informed; email: mark.truelove@bingleytowncouncil.gov.uk.

Reporting Point Responsibilities

All incidents must be recorded. The reporting point shall perform the following actions;

- Note the time, date and nature of incident together with a description and as much detail as appropriate on an Incident Response Form (in Appendix One below).
- Ensure the protection of any evidence and that a documented chain of evidence is maintained.
- Liaise with relevant authorities, individuals and the media where appropriate.
- Keep a note of all communications together with their date, time, who has been communicated with, and what the content and nature of communication was on the Incident Response Form.

Incident Response Plan

1. Assess the risk to individuals as a result of a breach; the following must be considered:
    a. The categories and approximate number of individuals concerned, and;
    b. The categories and approximate number of personal data records concerned, and;
    c. The likely consequences of the personal data breach, in particular consider if the impact results in a risk to the rights and freedoms of individuals.
    d. To help assess the risks refer to the Information Commissioner Office (ICO) website:
        i) https://ico.org.uk/for-organisations/report-a-breach/
        ii) https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

2. If the incident is deemed to be a notifiable incident the following actions must be taken:
    a. Within 72 hours of becoming aware of the incident (even if not aware of all the details yet):
    Call ICO: 0303 123 1113 – and provide the following information:
        - What has happened;
        - When and how the council found out about the breach;
        - The people (how many) that have been or may be affected by the breach;
        - What the council are doing as a result of the breach; and
        - Who else has been told.
    b. For reporting a breach outside normal working hours use the ICO Reporting Form: https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/

3. If the incident is deemed to result in a high risk to the right and freedoms of individuals:
    a. Within 48 hours the affected individuals must be informed by telephone, letter or email about the incident as there may be a need for them to take actions to mitigate immediate risk of damage to them.
    b. The individuals must be told in clear and plain language:
        i) The nature of the personal data breach;
        ii) A description of the likely consequences of the personal data breach;
        iii) A description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects;

iv) The name and contact details of the Town Clerk and Chair, from where more information can be obtained.

4. If the incident is not deemed to be notifiable:

a. Update the Council's Risk Register along with the outcome of the risk assessment.
b. Include the steps and evidence used to identify and classify the risk.
c. Include reasons why the incident is not deemed to result in a risk to the rights and freedoms of individuals.

5. Incident Review:

The Town Clerk and Chair will ensure that the incident is reviewed at the next appropriate Council meeting under an appropriate section of the agenda.

a. The Council/Finance and General Purposes Committee will consider whether discussion of the incident warrants exclusion of the press and public from the meeting during that discussion.
b. At that meeting, the Council should determine if there are any further actions that need to be assigned or completed as a result of the incident.
c. The Council may decide to refer further actions and to a committee, working group or external parties.
d. It should be noted that this final stage of the incident may require a review of this policy document.

Incident Response form

Date for review: Annually

If you have already spoken to a member of Bingley Town Council about this breach, please give their name:

……
……..

Report Type: (Please tick one)

- Initial report
- Follow-up report

What has happened?

Please tell us as much as you can about what happened, what went wrong and how it happened:

……
……
……
……
……
……
……..

Was the breach caused by a cyber incident?

- Yes
- No
- Don't know

How did you find out about the breach?

……
……
……
……

When did you discover the breach?

Date: ……
Time:……

When did the breach happen?

Date: ……
Time:……

Categories of personal data included in the breach (please tick all that apply):

- Data revealing racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Sex life data

- Sexual orientation data
- Gender reassignment data
- Health data
- Basic personal identifiers, eg name, contact details
- Identification data, eg usernames, passwords
- Economic and financial data, eg credit card numbers, bank details
- Official documents, eg driving licenses
- Location data
- Genetic or biometric data
- Criminal convictions offences
- Not yet known
- Other (please give details below)

……
……

Number of personal data records concerned?

……

How many data subjects could be affected?

……

Categories of data subjects (tick all that apply)

- Employees
- Users
- Subscribers
- Customers or prospective customers
- Children
- Vulnerable adults
- Not yet known
- Other (please give details below)

……
……

Potential consequences of the breach

Please describe the possible impact on data subjects, as a result of the breach. Please state if there has been any actual harm to data subjects:

……
……
……..

What is the likelihood that data subjects will experience significant consequences as a result of the breach?

- Very likely
- Likely
- Neutral – neither likely not unlikely
- Unlikely
- Very unlikely
- Not yet known

Please give details:
……
……

(Cyber incidents only) Has the confidentiality, integrity and/or availability of your information systems been affected?

- Yes
- No
- Don't know

(Cyber incidents only) If you answered yes, please specify (tick all that apply)

- Confidentiality
- Integrity
- Availability

(Cyber incidents only) Impact on your organisation

- High – you have lost the ability to provide all critical services to all users
- Medium – you have lost the ability to provide critical service to some users
- Low – there is no loss of efficiency, or a low loss of efficiency, and you can still provide all critical services to all users
- Not yet know

(Cyber incidents only) Recovery time

- Regular – you can predict your recovery time, with existing resources
- Supplemented – you can predict your recover time with additional resources
- Extended – you cannot predict your recovery time, and need extra resources
- Not recoverable – recovery from the incident is not possible, e.g. backups cannot be restored
- Complete – recovery is complete
- Not yet known

Had the staff member involved in this breach received data protection training in the last two years?

- Yes
- No
- Don't know

(**Initial reports only) If there has been a delay in reporting this breach, please explain why:**
……
……
……

(Follow-up reports only) Describe any measures you had in place before the breach with the aim of preventing a breach of this nature:
……
……
……

Describe the actions you have taken, or propose to take, as a result of the breach.
Include, where appropriate, actions you have taken to fix the problem, and to mitigate any adverse effect, e.g. confirmed data sent in error has been destroyed, updated passwords, planning information security training:
……
……
……

(Follow-up reports only) Outline any steps you are taking to prevent a recurrence, and when you expect they will be completed:
……
……
……

Have you told data subjects about the breach?

- Yes, we have told affected data subjects
- We are about to, or are in the process of telling data subjects
- No, they are already aware
- No, but we have decided not to
- We have not decided yet if we will tell them or not
- Something else (please give details below)

……
……

Have you told, or are you planning to tell any other organisations about the breach?
E.g. the police, other regulators or supervisory authorities. In case we need to make contact with other agencies:

- Yes
- No

- Don’t know

If answered yes, please specify:
……
……

About you

Organisation (data controller name):
……
……..

Registration organisation address:
……
……

Person making this report

In case we need to contact you about this report
Name:……
Email:……
Phone:……

Data protection officer

Or senior person responsible for data protection

- Same details as above

Name:……
Email:……
Phone:……

Sending this form

Initial report – if this is your initial report, please send your completed form to townclerk@bingleytowncouncil.gov.uk with ‘Personal data breach notification’ in the subject field.

Follow-up report – if this is a follow-up report, please reply to the email we sent you, attaching this completed form to it. (Make sure you leave the subject line as it is – this will ensure your follow-up gets added to your case).

Or send by post to: Bingley Town Council, The Hub, Myrtle Place, Bingley, West Yorkshire, BD16 2LF.

We will contact you once the information provided has been assessed and then provide information about the next steps.

To view our Privacy Notice please go to:
https://bingleytowncouncil.gov.uk/documents/general-privacy-notice/?wpdmdl=231439&refresh=653a31726da611698312562