Borough Council of Wellingborough
Making Wellingborough a place to be proud of

Purpose

This policy sets out how Borough Council of Wellingborough (BCW) employees should deal with a personal data breach and what information requestors can expect from us.

Legal obligation and duty

Under GDPR, data controllers (the Council) and data processors (employees) are now subject to a general personal data breach notification system. GDPR makes it clear that when a security incident takes place, data processors and controllers should quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it.

GDPR imposes a duty on data controllers to report personal data breaches to their supervisory authority (the Information Commissioner's Office (ICO)). In order to fulfil these obligations data processors must report all breaches to the Governance Officer upon awareness of the breach. Timing is key as the Governance Officer has 72 hours, where feasible, to report the breach to ICO.

If there is likely to be a high risk of the breach adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay. This will facilitate decision-making about whether or not you need to notify the relevant supervisory authority and the affected individuals.

Definition of a data breach:

Whether accidental or deliberate, a personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, corruption, alteration, unauthorised disclosure of, or access to personal data; or where data is passed on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

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; and
- Loss of availability of personal data.

When a breach has occurred:

1. **Data processors must notify the Governance Office without undue delay after becoming aware of it.**
   This includes near misses – a breach where no personal data is concerned.
   Exemption: There are no exemptions under the GDPR for this.
   Observations:
   - All breaches will have to be reported.

2. **Obligation for data controllers to notify the supervisory authority without undue delay and, where feasible, not later than 72 hours after becoming aware of it.**
   Exemption: No reporting if the breach is unlikely to result in a risk to the rights and freedoms of natural persons.
   Observations:
   - When the timing obligation is not met, reasons will have to be provided to the supervisory authority (e.g. request from a law enforcement authority).

3. **Obligation for data controller/processor to communicate a personal data breach to data subjects.**
   - If the data controller is yet to do so, the supervisory authority may compel the data controller to communicate a personal data breach with affected data subjects without undue delay,* unless one of the three exemptions is satisfied. *

   Exemption - no reporting necessary if:
   - The breach is unlikely to result in a high risk for the rights and freedoms of data subjects;
   - Appropriate technical and organisational protection were in place at the time of the incident (e.g. encrypted data); or
   - This would trigger disproportionate efforts (instead a public information campaign or "similar measures" should be relied on so that affected individuals can be effectively informed).

**the need to mitigate an immediate risk of damage would call for a prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar data breaches may justify more time for communication.*

Assessing the breach

When a personal data breach has occurred, the council need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then the Governance Officer must notify the ICO; if it's unlikely then it does not need to be reported. If the breach is not reported the reason must be justified and documented.

In assessing risk to rights and freedoms, it's important to focus on the potential negative consequences for individuals. Recital 85 of the GDPR explains that:

"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."

This means that a breach can have a range of adverse effects on individuals, which includes emotional distress, and physical and/or material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. This will need to be assessed on a case by case basis, looking at all relevant factors.

On becoming aware of a breach, you first should try to contain it, and then assess the potential adverse consequences for individuals (based on how serious or substantial these are) and how likely they are to happen.

To do list

Processors:

When reporting a breach, you must provide the below information to the Governance Officer:

- ✓ a description of the nature of the personal data breach including, where possible:
  - The categories and approximate number of individuals concerned;
  - The categories and approximate number of personal data records concerned;
- ✓ where more information can be obtained;
- ✓ a description of the likely consequences of the personal data breach; and
- ✓ a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

If at the time the breach is identified the above information is not available, information may be provided in phases, as long as this is done without undue further delay.

The investigation should be prioritised, given adequate resources, and expedited urgently. The ICO should still be notified upon awareness of the breach and further information submitted as soon as possible. This should be accompanied by an explanation as to the delay and an indication of when further information is expected to be submitted.

The Governance Officer on behalf of the data controller (BCW) will:

- Maintain an internal breach register regardless of whether notification is required.
- Record near misses.
- Advise if the affected data subjects (the individual whom the personal data relates to) need informing.
- Assess whether there are any additional notification obligations under other laws for example:
  - Notify the ICO of any personal data breach within 24 hours under the Privacy and Electronic Communications Regulations (PECR).
  - If a UK trust service provider - within 24 hours under the Electronic Identification and Trust Services (eIDAS) Regulation via the eIDAS breach notification form
  - If an operator of essential services or a digital service provider, you will have incident-reporting obligations under the NIS Directive.
- Record any reasons for not reporting a breach.

- Consider whether any third parties need informing, such as the police, insurers, professional bodies, or bank or credit card companies who can help reduce the risk of financial loss to individuals.
- Investigate whether or not the breach was a result of human error or a systemic issue and assess how a recurrence can be prevented – better processes, further training or other corrective steps.
- Ensure that lessons learned are recorded and the appropriate action is taken.

When to inform individuals of a breach:

If a breach is likely to result in a high risk to the rights and freedoms of individuals, those concerned must be informed directly as soon as possible without undue delay.

A 'high risk' means the threshold for informing individuals is higher than for notifying the ICO. The severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring will need to be assessed by the relevant service area. If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, then again the risk is higher. Those affected will need to be promptly informed, particularly if there is a need to mitigate an immediate risk of damage to them. This will help individuals take steps to protect themselves from the effects of a breach.

What to tell the individuals:

1. The nature of the personal data breach must be described in clear and plain English, including the name and contact details of your data protection officer (if your organisation has one) or other contact point where more information can be obtained.
2. A description of the likely consequences of the personal data breach.
3. 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.
4. That the ICO may be notified.
5. Advise individuals that if they are unhappy with the above BCW will consider it under our complaints process at the highest level via stage 2, which will be dealt with by a senior staff member.

Officers must prepare a statement detailing a summary of the conversation or correspondence with the individual concerned. This must then be sent to the Governance Officer to keep on file.

Failure to notify

Failing to notify a breach when required to do so and non-compliance can lead to an administrative fine up to €10,000,000 or, in case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Glossary

Personal Data	Means any information relating to an identified or identifiable natural person, who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
Special Category Data	▪ racial or ethnic origin; ▪ political opinions; ▪ religious or philosophical beliefs; ▪ trade union membership; ▪ physical or mental health or condition; ▪ sex life or sexual orientation.
Data Controller	The Borough Council of Wellingborough which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Data Processor	The Borough Council of Wellingborough (and its employees), or another agency or body to which the personal data are disclosed, whether a third party or not.
Supervisory authority	The governing body – Information Commissioner's Office (ICO).
Pseudonymisation –	The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
Individual concerned	The person the information relates to also known as the data subject and natural person.
Exemption	An exception to the rule.