**Downham West Parish Council**

**General Data Protection Regulation (GDPR)**

# PERSONAL DATA BREACHES POLICY

**Adopted 16th July 2018**

**Reviewed 15th May 2023**

**Personal Data Breach**

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. The Council must do this within 72 hours of becoming aware of the breach, where feasible.

If the breach is likely to result in a high risk of adversely affecting individuals’ rights and freedoms, the Council must also inform those individuals without undue delay.

The Council must keep a record of any personal data breaches, regardless of whether it is required to notify (see Appendix).

***Preparing for a personal data breach***

*☑  We know how to recognise a personal data breach.*

*☑  We understand that a personal data breach isn’t only about loss or theft of personal data.*

*☑  We have prepared a response plan for addressing any personal data breaches that occur.*

*☑  We have allocated responsibility for managing breaches to a dedicated person or team.*

*☑  Our staff know how to escalate a security incident to the appropriate person or team in our organisation to determine whether a breach has occurred.*

***Responding to a personal data breach***

*☑  We have in place a process to assess the likely risk to individuals as a result of a breach.*

*☑  We know who is the relevant supervisory authority for our processing activities.*

*☑  We have a process to notify the ICO of a breach within 72 hours of becoming aware of it, even if we do not have all the details yet.*

*☑  We know what information we must give the ICO about a breach.*

*☑  We have a process to inform affected individuals about a breach when it is likely to result in a high risk to their rights and freedoms.*

*☑  We know we must inform affected individuals without undue delay.*

*☑  We know what information about a breach we must provide to individuals, and that we should provide advice to help them protect themselves from its effects.*

*☑  We document all breaches, even if they don’t all need to be reported.*

**What is a personal data 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.

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.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

Recital 87 of the GDPR makes clear that when a security incident takes place, the Council should quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the ICO if required.

**What breaches do we need to notify the ICO about?**

When a personal data breach has occurred, the Council needs to establish the likelihood and severity of the resulting risk to people’s rights and freedoms. If it is likely that there will be a risk then the Council must notify the ICO; if it is unlikely then the Council doesn’t have to report it. However, if the Council decides it does not need to report the breach, the Council needs to be able to justify this decision and it should be documented.

In assessing risk to rights and freedoms, it is 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 include emotional distress, and physical and 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. The Council needs to assess this case by case, looking at all relevant factors.

So, on becoming aware of a breach, the Council should try to contain it and assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen.

For more details about assessing risk, please see section IV of the Article 29 Working Party guidelines on personal data breach notification.

**What role do processors have?**

If the Council uses a data processor, and this processor suffers a breach, then under Article 33(2) it must inform the Council without undue delay as soon as it becomes aware.

This requirement allows you to take steps to address the breach and meet your breach-reporting obligations under the GDPR.

If the Council uses a processor, the requirements on breach reporting should be detailed in the contract between the Council and its processor, as required under Article 28.

**How much time do we have to report a breach?**

The Council must report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it. If the Council takes longer than this, it must give reasons for the delay.

Section II of the Article 29 Working Party Guidelines on personal data breach notification gives more details of when a controller can be considered to have “become aware” of a breach.

**What information must a breach notification to the supervisory authority contain?**

When reporting a breach, the GDPR says you must provide:

* a description of the nature of the personal data breach including, where possible:
	+ the categories and approximate number of individuals concerned; and
	+ the categories and approximate number of personal data records concerned;
* the name and contact details of the data protection officer (if the Council has one) or other contact point 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.

**What if we don’t have all the required information available yet?**

The GDPR recognises that it will not always be possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it. So Article 34(4) allows the required information in phases, as long as this is done without undue further delay.

However, the ICO expects controllers to prioritise the investigation, give it adequate resources, and expedite it urgently. The Council must still notify the ICO of the breach when it becomes aware of it, and submit further information as soon as possible. If the Council knows it will not be able to provide full details within 72 hours, it is a good idea to explain the delay and tell the ICO when the information is expected to be submitted.

**How do we notify a breach to the ICO?**

The ICO’s personal data breach helpline can offer advice about what to do after experiencing a personal data breach, including how to contain it and how stop it happening again. The ICO can also offer advice about whether the Council needs to tell the data subjects involved.

**To report a breach, call the ICO helpline 0303 123 1113**; normal opening hours are Monday to Friday between 9am and 5pm (closed after 1pm on Wednesdays for staff training). The ICO will record the breach and give advice about what to do next.

### What information will I need to provide?

The ICO will need to know:

* what has happened;
* when and how the Council found out about the breach;
* the people that have been or may be affected by the breach;
* what the Council is doing as a result of the breach; and
* who the ICO should contact if it needs more information and who else the Council has told.

The ICO will send a copy of the information given.

**Can I report a breach online?**

If the Council has experienced a data breach and needs to report it to the ICO but the Council is confident that it has dealt with it appropriately, the Council can report it online. The Council may also want to report a breach online if it is still investigating and will be able to provide more information at a later date.

If the Council is reporting online, the telephone number of someone familiar with the breach should be given, in case the ICO needs to follow up any of the information provided.

Remember, in the case of a breach affecting individuals in different EU countries, the ICO may not be the lead supervisory authority. This means that as part of the breach response plan, the Council should establish which European data protection agency would be the lead supervisory authority for the processing activities that have been subject to the breach.

**When do we need to tell individuals about a breach?**

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the GDPR says the Council must inform those concerned directly and without undue delay. In other words, this should take place as soon as possible.

A ‘high risk’ means the threshold for informing individuals is higher than for notifying the ICO. Again, the Council will need to assess both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring. 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. In such cases, the Council will need to promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach.

If the Council decides not to notify individuals, it will still need to notify the ICO unless it can demonstrate that the breach is unlikely to result in a risk to rights and freedoms. The Council should also remember that the ICO has the power to compel the Council to inform affected individuals if it considers there is a high risk. In any event, the Council should document its decision-making process in line with the requirements of the accountability principle.

**What information must we provide to individuals when telling them about a breach?**

The Council needs to describe, in clear and plain language, the nature of the personal data breach and, at least:

* the name and contact details of the data protection officer (if the Council has one) or other contact point 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 and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

**Does the GDPR require us to take any other steps in response to a breach?**

The Council should ensure that it records all breaches, regardless of whether or not they need to be reported to the ICO.

Article 33(5) requires the Council to document the facts relating to the breach, its effects and the remedial action taken. This is part of the Council’s overall obligation to comply with the accountability principle, and allows the ICO to verify the Council’s compliance with its notification duties under the GDPR.

As with any security incident, the Council should investigate whether or not the breach was a result of human error or a systemic issue and see how a recurrence can be prevented – whether this is through better processes, further training or other corrective steps.

**What else should we take into account?**

The following are not specific GDPR requirements, but the Council may need to take them into account when it has experienced a breach.

The Council may also need to consider notifying third parties such as the police, insurers, professional bodies, or bank or credit card companies who can help reduce the risk of financial loss to individuals.

The European Data Protection Board, which will replace the Article 29 Working Party, may issue guidelines, recommendations and best practice advice that may include further guidance on personal data breaches. The Council should look out for any such future guidance. Likewise, the Council should be aware of any recommendations issued under relevant codes of conduct or sector-specific requirements that the Council may be subject to.

**What happens if we fail to notify?**

Failing to notify a breach when required to do so can result in a significant fine up to 10 million euros or 2 per cent of global turnover. The fine can be combined with the ICO’s other corrective powers under Article 58.