WCBC Schools: Data Breach Policy - St Peter's CiW Primary School

The General Data Protection Regulations (GDPR) has introduced a duty on all schools to report certain types of personal data breaches to the Information Commissioner's Office (the ICO).

The ICO define a personal data breach as:

"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."

Types of Breach

Data protection breaches could be caused by a number of factors, including:

- Loss or theft of pupil, staff or governing body data and/ or equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Equipment Failure;
- Poor data destruction procedures;
- Human Error;
- Cyber-attack;
- Hacking.

It is important that all school staff are able to identify a data breach when it occurs, and know the correct procedure for dealing for such an event – such as to whom the breach should be reported, and who will potentially pass the information onto the ICO. All school staff will receive the appropriate training, to ensure they are able to deal with a data breach in compliance with GDPR requirements.

Reporting a breach to the ICO will not be required on every occasion – the school Data Protection Officer (DPO), along with the school, will assess the breach, to decide whether it needs to be reported. GDPR states that breaches only need to be reported if they pose **a risk to the rights and freedoms of those affected** – examples of which include those breaches which could lead to:

- discrimination,
- financial loss
- identity theft or fraud, or
- reputational damage.

The school Data Protection Officer can be contacted via the local authority:

Email: SchoolsDPO@wrexham.gov.uk

The following steps should be followed by school staff when dealing with a potential data breach:

1. **Identifying the breach**

As soon as a data breach is identified, the relevant member of staff should inform the Headteacher immediately.

2. **Reporting the breach**

The Headteacher will then contact the school Data Protection Officer, to advise them of the breach. From the point of notification, the DPO has 72 hours to notify the ICO of the breach if it is deemed sufficiently high risk.

The Headteacher should also advise the Chair of Governors as soon as possible.

3. **Assessing the breach**

To assess the severity of the risk, the school need to complete the local authority's 'Data Security Incident Report' forms (Forms A and B), and return it to the Data Protection Officer. The forms will be provided from the authority at this stage. If required, the DPO can visit the school to assist with completing the form.

The DPO will review the report, and assess the featured scoring system. If the breach is deemed as sufficiently high-risk, the DPO will forward details of the breach to the ICO.

4. **Managing the breach**

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the GDPR says you must inform those concerned **directly and without undue delay**. If such contact isn't possible, for example if contact details for the subject aren't held by the school, a public notice would be sufficient, for example on the school website.

The school will give clear and specific advice to an individual on what they can do to protect themselves, and what the school is able to do to help them. The notification should include a description of how and when the breach occurred and what data was involved. Include details of what you have already done to mitigate the risks posed by the breach

This contact will not be necessary if appropriate if the school have adequate protective measures in place, such as encryption, to eliminate risk to data subjects.

All reasonable attempts will be made by the school to recover the data involved.

The school will keep a record of the reporting of the potential data breach in their Data Breach register. The record will include:

- the facts relating to the breach,
- the effects of the breach; and
- the remedial actions taken since the breach took place.

Records of all data breaches will be kept, regardless of whether the breach was reported to the ICO, in line with GDPR 'accountability' requirements.

5 Reporting the data breach

The Data Protection Officer will need to provide the following information to the ICO when reporting the data breach:

- a description of the nature of the data breach, including, where possible, the approximate number of individuals and personal data regards concerned, and the categories of the data;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken to deal with the data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

If the DPO is unable to fully investigate the breach within 72 hours to understand why it has happened, they will be able to submit information in phases, as a matter of priority. The DPO will advise the ICO of the situation to explain the delay, and also advise when they expect to have further information.

From the point that the breach is reported, the ICO will liaise with the School DPO to update them on their investigation. The DPO will keep the school advised of how the investigation is progressing.

Review and Evaluation

Once the initial aftermath of the breach is over, the Head Teacher and DPO should review both the causes of the breach and the effectiveness of the response to it. It should be reported to the next Governors meeting for discussion. If systemic or ongoing problems are identified, then an action plan must be drawn up to put these right.

Implementation

The Head Teacher should ensure that staff are aware of the requirements of this breach procedure. This should be undertaken as part of induction, supervision and ongoing training. This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance.