CEFN SAESON COMPREHENSIVE SCHOOL

DATA BREACH POLICY

1 Background

Data security breaches are increasingly common occurrences whether caused through human error or via malicious intent. As the amount of data and information grows and technology develops, there are new ways by which data can be breached. The School needs to have in place a robust and systematic process for responding to any reported data security breach, to ensure it can act responsibly and protect personal data which it holds.

2 Aim

The aim of this policy is to standardise the School's response to any data breach and ensure that they are appropriately logged and managed in accordance with the law and best practice, so that: incidents are reported swiftly and can be properly investigated

- incidents are dealt with in a timely manner and normal operations restored
- incidents are recorded and documented
- the impact of the incident is understood, and action is taken to prevent further damage
- the ICO and data subjects are informed as required in more serious cases
- incidents are reviewed, and lessons learned

3 Definition

Article 4 (12) of the General data protection Regulation ("GDPR") defines a data breach as:

"a breach of security leading to the unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed."

Cefn Saeson Comprehensive School is obliged under the GDPR to act in respect of such data breaches. This procedure sets out how the School will manage a report of a suspected data security breach.

The aim is to ensure that where data is misdirected, lost, hacked or stolen, inappropriately accessed or damaged, the incident is properly investigated and reported, and any
necessary action is taken to rectify the situation.

A data security breach can come in many forms, but the most common are as follows:

- loss of theft of paper or other hard copy
- Data posted, emailed or fixed to the incorrect recipient
- Loss of theft of equipment on which data is stored
- Inappropriate sharing or dissemination-staff accessing information to which they are not entitled
- Hacking, malware, data corruption
- Information is obtained by deception or "blagging"
- Equipment failure, fire or flood

- Unescorted visitors accessing data
- Non-secure disposal of data

In any situation where staff are uncertain whether an incident constitutes a breach of Security, either report it to the Data Protection Officer (DPO) or the Senior Information Risk Owner (SIRO). If there are IT issues, such as the security of the network being compromised, IT should be informed immediately.

4 Scope

This School policy applies to all School information, regardless of format, and is applicable to all officers, members, visitors, contractors, partner organisations and data processors acting on behalf of the School. It is to be read in conjunction with the School's Information Security Policy.

5 Responsibilities

Information users

The GDPR applies to both Data Controllers (the School itself) and to Data Handlers. Therefore, all information users are responsible for reporting actual, suspected, threatened or potential information security incidents and for assisting with investigations as required, particularly if urgent action must be taken to prevent further damage.

Managers

Heads of Department are responsible for ensuring that staff in their area act in compliance with this policy and assist with investigations as required.

Lead Responsible Officers

Lead responsible officers (DPO, SIRO) will be responsible for overseeing management of the breach in accordance with the Data Breach Management Plan. Suitable further delegation may be appropriate in some circumstances.

6 Reporting a Breach

Internal

Suspected data security breaches should be reported promptly to the SIRO as the primary point of contact on 01639 791307 extension 3307, email: PowisA1@hwbmail.net

The report must contain full and accurate details of the incident including who is reporting the incident [and what classification of data is involved]. The incident report form should be completed as part of the reporting process. See Appendix 1. Once a data breach has been reported an initial assessment will be made to establish the severity of the breach. See Appendix 2.
All data security breaches will be centrally logged by the SRIO to ensure appropriate oversight in the types and frequency of confirmed incidents for management and reporting purposes.

External
Article 33 of the GDPR requires the School as data controller to notify the ICO only when the breach
"*is likely to result in a risk to the freedoms and rights of natural persons*". Such a breach also must be communicated to the data subject (with certain exceptions). Notification must be made "*without undue delay*" and within 72 hours of becoming aware of it. If the School fails to do this, it must explain the reason for the delay.

Article 33(5) requires that the School must maintain documentation on data breaches, their nature and remedial action taken.

A report to the ICO must contain information as to the nature of the breach, categories of data, number of data records, number of people affected, name and contact details of DPO, likely consequences of the breach and action taken.

7 Data Breach Management Plan

The School's response to any reported data security breach will involve the following four elements.

A. Containment and Recovery
B. Assessment of Risks
C. Consideration of Further Notification
D. Evaluation and Response

Each of these four elements will need to be conducted in accordance with the checklist. An activity log recording the timeline of the incident management should also be completed.

NB. This reflects current guidance from the ICO, which is likely to change.

8 Disciplinary

Officers, members, contractors, visitors or partner organisations who act in breach of this policy may be subject to disciplinary procedures or other appropriate sanctions.

9 Review

This document shall be subject to annual review by the DPO/SIRO.

10 References

- The GDPR
  https://gdpr-info.eu/

- ICO GUIDANCE ON DATA BREACHES
https://ico.org.uk/media/fororganisations/documents/1562/guidance_on_data_security_breach_management.pdf