CWMBRAN HIGH SCHOOL

Information Data Loss Policy

CCTV Policy: November 2023

NEXT REVIEW: November 2024

Approved by IEB: 23 November 2023

Table of Contents

1. PURPOSE

Cwmbran High School is committed to ensuring that all personal data we process including that of employees, pupils, parents/carers and visitors is managed appropriately and in compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Sometimes an incident may occur whereby information/data is accidentally disclosed to unauthorised persons, or lost, or stolen or copied/extracted as a result of a targeted attack. The school have processes in place to ensure that personal data breaches are identified, reported and dealt with and where appropriate reported to the Information Commissioners Office (ICO) and affected individuals.

2. SCOPE

This policy and procedure document lays out the actions to follow once a breach has occurred and applies to all information held by the school or held on behalf of the school. This includes information in paper and electronic formats, inclusive of CCTV and voice recordings.
This document applies to the following:
Governors, employees, whether office based or working via remote access, including contractors, volunteers, agency workers and partner organisations operating on behalf of the school.

3. AIMS AND OBJECTIVES

Legislation places a responsibility on the school to protect the information it holds.

- This involves ensuring the maintenance and protection of the security and confidentiality of information held by the school.
- To minimise the risk of information/data loss through appropriate technical measures
- To educate and raise awareness amongst staff of information/data loss procedures
- To meet ICO compliance with regard to notification of breaches and GDPR regulations.

4. RESPONSIBILITIES

Governors / Head teacher	• Have overall responsibility for compliance with this policy.
Systems and Operations Manager	• Will have responsibly for reporting incidents involving IT to technical/security staff within the SRS and incidents involving breaches of personal data to the Torfaen Data Protection Team and liaise with the departments as appropriate • Will update the Governors on significant breaches immediately and where necessary the system administrator. • Where appropriate and in conjunction with the data protection team (DP Team) will notify breaches to the Information Commissioners Office (ICO) within 72 hours in order to comply with the UK GDPR and the Data Protection Act 2018 • Will where appropriate and in conjunction with the DP Team notify the individual of the breach of personal information • Will, when necessary, enlist the involvement of police and internal departmental support if following on from an investigation, the likelihood of legal, civil or criminal action is established and where information gathered is treated as potential evidence in a disciplinary, criminal or civil action. All evidence, in any format will be retained securely.

	• Will be responsible for initiating disciplinary action where required by referring to the incident and will have access to the information collected as part of the investigation • Will notify the DP Team after corrective measures have been implemented to close down the data loss incident
All staff	• Have responsibility to be aware of potential security incidents as defined in this policy and to follow procedure in the event of a breach of data • Are required to report all incidents, both actual and suspected as soon as possible but no later than 24 hours to the Systems and Operations Manager. Failure to report such incidents may result in disciplinary action. • Relevant personnel are required to fully support the Systems and Operations Manager & the DP Team in reporting and dealing with incidents. • Undertake mandatory data protection training • All staff are aware of the rights of the individual under UK GDPR regulations these are: ○ The right to be informed ○ The right of access ○ The right to rectification ○ The right of erasure ○ The right to restrict processing ○ The right to data portability ○ The right to object Rights in relation to automated decision making and profiling.

5. LEGISLATION & KEY REFERENCE DOCUMENTS

(Please note this list is not exhaustive)

- General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Human Rights Act (1998)
- Privacy and Electronic Communications Regulations (2003)
- Computer Misuse Act 1990

POLICIES

- Data Protection Policy
- Acceptable Use Policy
- Password Policy

PROCEDURES

- Retention Guidelines

Other useful documents:

- **ICO Information Security Guide(link is external)**
- **ICO Guidance on Personal Data Breaches(link is external)**

6. MONITORING AND REVIEW

The Governing Body and Systems and Operations Manager will monitor the implementation of this policy and monitor reviews.

This policy will be subject to review when any of the following conditions are met:

- Content errors or omissions are highlighted.
- Where another standard/guidance issued conflicts with the information in this policy.
- There will be an initial 1-year review from policy implementation.
- Thereafter reviews will be scheduled on a 3-year basis from the date of approval of the current version.

7. COMPLIANCE

Failure to comply with this Policy could result in disciplinary action. This could result in termination of employment and in serious cases individuals being prosecuted under the UK General Data Protection Regulation.

- Cwmbran High School is its own Data Controller and is registered with the ICO. If you would like to exercise any of the GDPR rights outlined in this policy or make a complaint in relation to how your data has been handled you should contact:

Tom Herbert
Systems and Operations Manager
Cwmbran High School
Tom.herbert@chs.schoolsedu.org.uk

You may also contact the Information Commissioner (ICO). The Information Commissioner's Office (Wales) can be contacted at: The Information Commissioner's Office (Wales), 2nd Floor, Churchill House, Churchill Way, Cardiff, CF10 2HH. Telephone 0330 414 6421 e-mail Wales@ico.org.uk

APPENDIX 1 –

SCHOOL-IGFM001 Information Data Loss Form v2.docx

APPENDIX 2 –

SCHOOL - IGFM014 Incident Containment Form v4.docx

INFORMATION DATA LOSS PROCEDURE

1.0 What is Personal Data

- **Personal data is** information relating to natural persons who:

  - can be identified or who are identifiable, directly from the information in question; or who can be indirectly identified from that information in combination with other information.
  - Personal data may also include special categories of personal data or criminal conviction and offences data. These are considered to be more sensitive and you may only process them in more limited circumstances as they are afforded extra protection. Special category data is:
  - personal data revealing **racial or ethnic origin**;
  - personal data revealing **political opinions**;
  - personal data revealing **religious or philosophical beliefs**;
  - personal data revealing **trade union membership**;
  - **genetic data**;
  - **biometric data** (where used for identification purposes);
  - data concerning **health**;
  - data concerning a person's **sex life**; and
  - data concerning a person's **sexual orientation**.

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.

For the purpose of this document a data security breach includes both confirmed and suspected incidents

Examples of breaches are as follows – please note this list is not exhaustive –

- human error in dealing with personal information including both electronic and paper

  An individual who becomes aware of an actual, suspected or potential Information/Data loss must report it immediately **but no later than 24 hours** to the Systems and Operations Manager and the Data Protection Team at DPA@torfaen.gov.uk and complete the Information/Data Loss Form (see Appendix 1)

- access by an unauthorised third party to both electronic equipment and paper
- loss of data through loss or theft of equipment on which data is stored. The loss of data through school assets, such as laptops, storage devices, and mobile devices. These must be reported to the Systems and Operations Manager and Data Protection Team DPA@torfaen.gov.uk and also to the Security Team in the Shared Resource Services (SRS) security@srswales.com this will ensure that devices can be disabled immediately

  - In cases of stolen assets please contact the police to obtain a crime reference number.

- hacking attack, phishing attack on the ICT systems
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it.
- Any individual who becomes aware of an actual, suspected or potential Information/Data loss via a phishing email or suspect they have been the victim of a cyber attack, report immediately to the Systems and Operations Manager and email security@torfaen.gov.uk and dpa@torfaen.gov.uk or
- Unauthorised access to school areas
- Any complaints from a member of the public, third party or employee, where they suspect theirs or another's data may have been breached, or privacy rights have not been followed must be reported immediately to the Systems and Operations Manager who will then report to the Data Protection Team DPA@torfaen.gov.uk

2.0 Reporting a Data Breach

Breach reporting is encouraged throughout the school and staff are expected to seek advice if they are unsure as to whether the breach should be reported. If you know or suspect a personal data breach has occurred or may occur you should:

1.	Contact the Systems and Operations Manager and data protection team (DP) DPA@torfaen.gov.uk immediately. The DP team will log the breach in the data protection log and provide you with advice and paperwork.
2.	Where possible try to contain the breached data and confirm deletion via an email/screenshot. Send a containment form to the recipient. See Appendix 2
3.	Systems and Operations Manager and DP team will assess the breach risk and impact
4.	Person that caused the breach will complete a data breach form See Appendix 1

5.	Once assessed (point 3) Systems and Operations Manager or DP team may notify data subjects affected by the breach
6.	Once assessed (point 3) if high risk to individual DP team will notify the ICO
7.	Once assessed DP team may notify other appropriate parties of the breach;
8.	School to take mitigating steps to prevent future breaches and update staff and DP team
9.	Once finalised, return all paperwork and inform DP team who will then close down the breach in the log.

3.0 Assessing the Risks/ When Does It Need To Be Reported?

The Systems and Operations Manager and DP team will carry out the initial assessment of the breach and consider whether the event meets the UK GDPR criteria to be reported.

Factors to be considered (these factors are not exhaustive):

- The type of breach, who it affects
- The nature, volume and sensitivity of the personal data breached
- How easy it is to identify individuals
- The potential consequences for individuals – could its disclosure be harmful to the individual it relates to, physical risk, reputational, financial, fraud
- If data has been lost or stolen is the data encrypted, can it be restored or recreated

4.0 Reporting to the ICO

- The UK GDPR places a duty on all organisations to report certain types of data breach to the Information Commissioner's Office (ICO)
- In the case of a personal data breach, if the breach were to result in a high risk to the rights and freedoms of individuals, which include emotional distress, physical and material damage and concerns over safety. The Systems and Operations Manager in liaison with the DP team shall without undue delay and, where feasible, no later than 72 hours after becoming aware of breach, notify the ICO. A reason for the delay, if notification is not within 72 hours, is required along with the notification. There is no need to notify the ICO if there is not a high risk to persons' rights and freedoms.
- Failing to notify the ICO of a breach when required to do so can result in a heavy fine of up to £8.7 million or 2 per cent of global turnover. The fine can be combined with the ICO's other corrective powers under Article 58.