Torfaen County Borough Council

Griffithstown Primary School

Information/Data Loss Policy

Version 4.0 Live

DOCUMENT CONTROL

Title:	**Information/Data Loss Policy**		
Document Owner:	**Senior Information Risk Owner** (SIRO)		
Document Author:	**Sharon Clifford**		
Reference:	**IG012**	**Retention Period:**	**Until next review**
Document Classification:	Official	**Location:**	SWOOP
Version / Status:	Live	**Approved by:**	ICT Heads March 2026
Current Issue Date:	January 2026	**Next Review Date:**	January 2029

REVISION HISTORY

Issue Date	Version / Status	Reason for Change	Changed By:
October 2019	1.0 Live	Policy Implementation	Sue Bullock
June 2021	1.1 Live	Updated VC from Draft to Live and amended DP Legislation- full review still required therefore review date unchanged	Sharon Clifford
January 2026	1.2 Live	Policy moved into new template and legislation updated	Jessica Stokes-Jones

TABLE OF CONTENTS

1. PURPOSE 4

2. SCOPE 4

3. AIMS & OBJECTIVES 4

4. RESPONSIBILITIES 5

5. LEGISLATION & KEY REFERENCE DOCUMENTS 7

6. MONITORING AND REVIEW 8

7. COMPLIANCE 9

1. PURPOSE

Griffithstown Primary School is legally required under Data Protection legislation (UK GDPR/Data Protection Act 2018/Data Use and Access Act (DUAA 2025)) to ensure the security and confidentiality of the information/data it processes of those who engage and work with the School e.g. students, visitors, governors and employees.

An information data loss or data incident is a situation where the School has lost control of the processing of data containing personal and/or confidential/sensitive information. Furthermore, the loss of this data has the potential to cause distress and/or harm to the individual, whose data has been compromised, or affect the commercial interests of third-party organisations.

Such incidents can occur where information/data is accidentally disclosed to unauthorised persons, damaged/destroyed (e.g. by fire/flood), corrupted, lost, stolen, or copied/extracted as a result of a targeted attack.

The School has a responsibility to mitigate against further recurrences of information data losses through implementation of appropriate measures. This policy should be read in conjunction with the suite of Information Governance policies on SWOOP notably Data Protection (IG007), Information Security (IG019) and Acceptable Use (IG006).

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 & OBJECTIVES

Legislation places a responsibility on the School to protect the information it holds. This will be achieved by:

- Minimising the risk of information/data loss through appropriate technical and procedural measures.
- Educating and raising awareness of information/data loss procedures.
- Adhering to the appropriate Records Management and Information Governance guidance
- Having robust processes in place to meet ICO compliance regarding notification of breaches and UK GDPR regulations.

4. RESPONSIBILITIES

Governors/ Head teacher	Have overall responsibility for compliance with this policy.
Headteacher/DP team	• Will have responsibly for reporting incidents involving IT to technical/security staff within the SRS and incidents involving breaches of personal data to the Data Protection Team DPA@Torfaen.gov.uk Incidents are reported as soon as possible, **but no later than 24 hours,** • 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 by the Head teacher, who will have sole responsibility for the authorising of access to other personnel as appropriate. • 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 Head teacher. Failure to

	report such incidents may result in disciplinary action. • Relevant personnel are required to fully support 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.

The most common examples of Data Loss include:

- Loss of documents that contain personal data: either sent to third parties or individuals. This could include emails sent to incorrect recipients, wrong addresses or not using the Bcc function.
- The destruction/deletion of information prior to its assigned destruction/retention date.
- Lack of access to data due to system errors/out of date software.
- Lost or stolen devices including BYOD (Bring your own Device) which **must** be reported to the Data Protection & Information Governance Team DPA@torfaen.gov.uk **and also** to the Security Team in the Shared Resource Services (SRS) Security@srswales.com to ensure that devices can be disabled immediately.

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

An individual who becomes aware of an actual, suspected or potential Information/Data loss, must complete the Information/Data Loss Form IGFM001 ((obtained from the School Lead for GDPR) and report it immediately to their line manager/supervisor and the Data Protection & Information Governance Team via email DPA@torfaen.gov.uk.

Whilst School staff may initiate an immediate investigation into the incident, this **must not** delay reporting to the Data Protection & Information Governance Team. They must use the Data Protection Incident Containment Form IGFM014

(obtained from the School Lead for GDPR) to ensure containment of the breached information.

Any complaints from a member of the public, third party or employee, where they suspect their or another's personal data may have been breached, or privacy rights have not been maintained, must be reported **immediately** to the Data Protection & Information Governance Team DPA@torfaen.gov.uk.

All Employees have a responsibility to be alert to potential security incidents and acknowledge that failure to report incidents may result in disciplinary action. Therefore, they should familiarise themselves with the guidance and relevant forms available from the School Lead for GDPR, seeking any clarity from the Data Protection & Information Governance team.

5. LEGISLATION & KEY REFERENCE DOCUMENTS

(Please note this list is not exhaustive)

The Council will abide by all relevant UK legislation and the following policies and procedures:

- UK GDPR (General Data Protection Regulation)
- The Data Protection Act (2018)
- The Data Use and Access Act (2025)
- The Copyright, Designs and patents Act (1988)
- The Computer Misuse Act (1990)
- The Health and Safety at Work Act (1974)
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Social Services & Well-being (Wales) Act 2014
- Children Act 2004 / 2019
- Equality Act 2010
- Crime and Disorder Act 1998
- Privacy and Electronic Communications (EC Directive) Regulations 2003 (amended 2019)PECR
- Welsh Language Standards

TCBC POLICIES

- IG007 Data Protection Policy
- IG001 Information Governance & Information Management Framework
- IG002 Information Governance Strategy
- IG003 Information Governance Policy

- IG006 Acceptable Use Policy
- IG019 Information Security Policy
- IG017 Information Sharing Policy
- IG013 Records Management Policy
- IG020 Retention Policy
- IG022 Information Secure Destruction Policy
- IG021 Requests for Information Policy
- IG011 Clear Desk Policy
- IG016 FOI Policy
- IG024 EIR Policy
- IG008 Password Policy
- IG023 BYOD Policy
- IG009 Social Media Policy
- Dignity at Work Policy
- IG101 Offsite Archive & Retention Policy
- IG025 Email Policy
- IG026 Version Control Policy

TCBC PROCEDURES

- IG007 (A) Data Protection Procedures
- IG101 (A) Offsite Archive & Destruction Procedures
- IG021 (A)(B) Requests for Information Procedures
- IG008 (A)Password Construction Procedures
- IG020 (A)(B) Retention Schedule (on SWOOP)
- IG023 (A) BYOD Guidance
- IG006 (A) Acceptable Use Procedures
- IG025 (A) Email Procedures
- Social Media Guidance
- Code of Conduct for Employees

6. MONITORING AND REVIEW

The Governing Body and Head teacher 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.
The 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:

The Head teacher
Head.griffithstownprimary@torfaen.gov.uk

If you are not satisfied you may also contact the Data Protection and Information Governance Office of Torfaen County Borough Council DPA@torfaen.gov.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

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 Head teacher 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 Head teacher 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 Head teacher and email security@torfaen.gov.uk and dpa@torfaen.gov.uk
- 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

Head teacher 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 Head teacher 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.	Head teacher 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) Head teacher 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.	Head teacher, and Governors 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 Head teacher 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 Headteacher 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.