Griffithstown Primary School
Information Security Policy

Version 2.0 Live

DOCUMENT CONTROL

Title:	**INFORMATION SECURITY POLICY**		
Document Owner:	**HEADTEACHER**		
Document Author:			
Reference:	**SCHOOL-IG009**	**Retention Period:**	Until next review
Document Classifi-cation:	Official	**Location:**	
Version / Status:	Live	**Approved by:**	29.04.2020 PSJCC SCHOOL /BOARD GOVENORS
Current Issue Date:	April 2020 July 2025	**Next Review Date:**	April 2024 July 2029

REVISION HISTORY

Issue Date	Version / Status	Reason for Change	Changed By:
April 2020	1.0	Policy implementation	A Price
April 2021	1.0	Change to UK GDPR	AP
June 2024	2.0	Review of policy	KE
July 2025	2.0	Approved of Policy by PSJCC	KE

TABLE OF CONTENTS

1. **PURPOSE**

   Information is a vital asset and must be afforded the necessary security required so that Schools can maintain services and carry out functions. Schools create, collect, process, share and dispose of information daily and must comply with legal, regulatory and contractual obligations to ensure the confidentiality, integrity and availability of this information. It can be electronic, physical and verbal (e.g. conversations, presentations, CCTV, Teams recordings, texts, instant messaging Apps, social media) and must be protected against risks whether natural, accidental or deliberate which includes poor processes or security.

   As new and emerging technologies become widely available to assist with remote working it is essential that staff recognise possible risks and their responsibilities in protecting and securing this information.

   The purpose of this Information Security Policy is to define the school's responsibility for the security of all the information it holds, and to ensure it is kept safe and used only in the appropriate way.

   This policy will set out the measures taken to protect information held by the school. The policy will assist the school and its employees to abide by and adhere to all current UK and EU legislation as well as a variety of regulatory and contractual requirements.

   Information Security can be defined as the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

   Staff are referred to the Data Protection Policy and Acceptable Use Policy for further information. These policies are designed to protect personal data – and can be found on the school website.

2. **SCOPE**

   The policy applies to all information created, received, maintained and held in all formats by the school and applies to:

   - Governors, employees, whether office based or working via remote access, contractors, supply teachers, volunteers, agencies and partner organisations operating on behalf of the school.

3. **PRINCIPLES**

   The school has many responsibilities as a data controller and this policy will ensure adherence to legislation including the UK General Data Protection Regulations *Regulation* and Data Protection Act 2018. This in turn will protect the security of the data of our pupils and staff.

4.   AIMS & OBJECTIVES

Torfaen County Borough Schools' Information Technology Systems are overseen by the Shared Resources Service. As a school we sign up to an SLA with the SRS.

The SRS and Head teacher will have the overall responsibility for monitoring information security inclusive of internal and external suppliers and sub-contractors.

All information stored on our IT Systems and our paper records shall be available only to members of staff with legitimate need for access and shall be protected against unauthorised access and/or processing and against loss and/or corruption.

This policy will contribute to a system of controls that supports Information Security across schools to protect the security of the data we process by:

- Providing a framework for establishing suitable levels of information security for all School information systems and to mitigate risks associated with theft, loss, misuse, damage or abuse of systems and providing compliance with any legal and contractual requirements around information security
- Ensuring that all users understand their own responsibility for protecting the confidentially and integrity of the data they handle
- Advising and protecting both the employee/user and the School from liability or damage through inappropriate use which exposes the School to risks including virus attacks, the compromising of network systems and services, and legal issues to which non-compliance could lead to a disciplinary investigation against the user
- Providing Data Protection training to staff and raising awareness of Data Protection Legislation via mediums such as induction, policies, bulletins
- Embedding Data Protection principles into processes to strengthen internal controls for all systems containing School information or personal data
- Incorporating information security at every stage of development for new systems /projects using Data Protection Impact Assessments (DPIA) or Data Protection Risk Assessments (DPRA) and the appropriate route e.g. Projects/Software Approval Process
- Ensuring a system of control is in place to prevent staff accessing unapproved software/Apps/portals/platforms
- Implementing robust procedures to prevent unauthorised access to information held in any system or physical location
- Advising staff how to respond to an incident or suspected incident

Data Breaches/Loss of Data

The School must manage the security of its information and must make every effort to avoid security and data breaches. If you experience a Data Breach or Loss of Data you must inform the Head Teacher and the Data Protection and Information Governance team at DPA@torfaen.gov.uk immediately.

- You must make every effort to retrieve the information as soon as you are aware of the breach/loss
- Templates and guidance are available on SWOOP and assistance available from the Data Protection and Information Governance Team
- You must **not** contact the ICO directly as notification must be via the Data Protection Officer at Torfaen's Information Governance Team

For further help with Data Protection issues and your responsibilities as an employee, please refer to the relevant TCBC Policies listed at the end of this document.

Some simple steps are listed below to help you keep information safe:

- Ensure you double check the email address especially if using the autofill address facility
- When sending sensitive information externally you must ensure that security measures are implemented such as emailing with password-protected attachments, a link to the secure OneDrive area, ensuring that both sender and recipient email addresses are enabled to TLS 1.2 or above
- Check postal addresses and use recorded delivery where appropriate
- Check outgoing mail envelopes only contain the addressee's documents – ensure no other paperwork has become attached

When working at home/offsite – ensure you cannot be overheard, that your devices are secured, and screens cannot be viewed
- Do not save School data to a Drive/device (such as I Drive/OneDrive) that your colleagues cannot acces

IT Security

The School has processes in place to ensure access to information is managed via the User Access Forms, which are completed by line managers and managed through the SRS. Managers must ensure access is limited to only what is necessary or relevant for that role.

UARs must be completed as soon as possible to ensure that only appropriate and currently-employed staff, can access School systems – this includes the BYOD facility.

The Council undertakes monitoring of IT systems and has an IG006 Acceptable Use Policy to ensure that staff are aware of their responsibilities, as well as a IG008 Password Policy to comply with information security standards.

Staff must not access software/Apps/portals/platforms that have not been approved and must log a request through the Halo system.

Staff must use caution with email links and attachments as stated in the IG006 Acceptable Use policy. Phishing emails attempt to trick you into clicking on a link that criminals will use to steal personal information or download malware from the internet which may infect your device and the corporate network. These messages will often look legitimate and use official logos to try to convince you that the email is authentic.

If you are unsure if an email you have received is genuine, contact TCBC Security for advice security@torfaen.gov.uk and copy DPA@torfaen.gov.uk

SRS utilise a suite of tools to protect the systems and information used by the School, to reduce the effectiveness and impact of cyber-attacks including ransomware and anti-malware software.

If your computer is automatically shut down, this will mean the system has identified an issue. Contact SRS helpdesk on 01495 766366 immediately and they will guide you through the process - do not attempt to power up your laptop until you speak to the SRS.

Should a major security incident be detected, staff will be informed through approved communication channels and must not share this publicly

Please visit Cyber & Information Security - Swoop, the Intranet for Torfaen Employees on SWOOP for more advice

Physical Security

- The School adopts security controls throughout its buildings to ensure only the appropriate personnel have access to buildings and School equipment. Staff must **not** allow access to unauthorised personnel and should be confident to challenge anyone who requests access. This includes checking identification and **not** allowing 'tailgating'.

- Where Digital Door Locks are in operation – codes should be changed on a regular basis with assistance from the Site Management team

- Any loss of equipment must be reported immediately to SRS Security team security@srswales.com ICT Client team ICTClientTeam@torfaen.gov.uk and Data Protection & Information Governance team DPA@torfaen.gov.uk as well as a line manager. In the event of a workplace incident such as burglary/fire, the Premises Manager/keyholder will follow standard School procedure where equipment has been damaged/stolen

Sending and Sharing Information

Staff must **only** share information where they have clear authority or a legal obligation to do so and **only** share what is necessary. They should familiarise themselves with the IG021 Requests for Information Policy and IG021 (A) Request for Information Procedures for clarity, some of which is listed here:

When posting, emailing and faxing:

- If posting sensitive information, it should be sent recorded postal delivery for example, if responding to a subject access request
- When sending sensitive information externally you must ensure that security measures are implemented such as emailing with password-protected attachments, a link to the secure OneDrive area (HWB), ensuring that both sender and recipient email addresses are enabled to TLS 1.2 or above
- Check and double check the email address to minimise the risk of a data breach. Do **not** Reply All and ensure any conversation thread is not included unless necessary.
- Faxing should not be used for personal data. If it is the only means available, you must ensure some measures are in place so that the person collects the information immediately and confirms receipt

- Ensure contracts and/or sharing agreements are in place with partner organisations where regular sharing takes place and processes for doing so have been agreed
- Understand the types of Requests you may receive and from whom e.g. Police/Health/CCTV/WG/HMRC/solicitors/insurance companies
- Understand the difference between providing 'business as usual' information compared to a Rights Request
- Be aware that as a School we will also hold 'commercially sensitive' data such as contracts, financial information, staff data, and that building location data (such as storage or departments) as well as geo-location devices, can identify staff workplaces or shift patterns

Storage of data:

- The School enforces a clear desk policy where paper records and devices are stored securely
- When working at home or offsite, the appropriate precautions must be taken to ensure information and devices are secure and not accessible to others
- Ensure only approved software/Apps/portals/platforms are used as they may store school data
- Paper files should not routinely be removed from School buildings to work on at home
- Paper files that cannot be destroyed are held securely at the Offsite Archive facility until their designated Retention date when they are reviewed before secure disposal, managed through the appropriate procedure
- Where information systems reach end of life, they must be decommissioned or have the appropriate security controls enforced and where applicable, information migrated to its replacement with assistance from SRS

5. RESPONSIBILITIES
Governors and Head teacher
Will have overall responsibility to ensure that relevant security standards are adhered to ensure that all staff and governors are aware of school policies and procedures.

Head teacher
Will be responsible for monitoring information security throughout the School, ensuring there are relevant policies and procedures in place that underpin Information Security and that staff follow these policies and procedures.
Will work with the Shared Resource Service to ensure IT data and information is protected and will be responsible for the information systems both manual and electronic that support the School.
Will work with and report breaches to the Data Protection Officer of TCBC and upon advisement and consultation inform Information Commissioner.

Work with the Shared Resource Service to ensure data and information is protected and will be advised of IT security breaches from the SRS.

Head teacher/Business Manager/Bursar

Will ensure all policies and procedures are kept up to date and all staff are aware of these processes.

Will undertake Data Protection Impact Assessment with advice from the Data Protection and Information Governance Office in line with the legal requirement within the UK GDPR/DPA when:

- Processing is likely to result in a high risk to individuals
- A new IT system is procured
- New types of data are collected or more intrusive methods and purpose for collecting the data occurs such as systematic and extensive profiling
- Ensuring contracts and/or sharing agreements are in place with partner organisations

Shared Resource Service (SRS)

Through acceptance of school SLA agreements, the SRS will protect school IT systems by:

- Encryption:
  All Laptops are encrypted using BitLocker
- Securing laptops:
  Staff are guided on how to keep laptops secure through the Council's/Schools Acceptable Use Policy, Password Policy and Procedures
- Testing:
  The Shared Resource Service will conduct annual health checks on IT systems. All servers and networking equipment is subject to vulnerability testing as part of the same annual health check.

All Staff

Will ensure the security of information when sharing, and will:

- Undertake security checks at point of contact with customers
- Ensure contracts and/or sharing agreements are in place with partner organisations
- Only share what is necessary
- Be familiar with policies surrounding sharing of information such as Request for Information Policy and Procedure, Subject Access Request Procedure,
- Be familiar with the different types of information requests that could be received eg Police Request, Education Record Requests.

When posting, emailing and faxing:

- Consider sending sensitive information by recorded postal delivery for example if responding to a subject access request.

- All staff are responsible for ensuring that sufficient measures are put in place when sending personal/special category (personal/ sensitive) data. Information between school and internal departments of Torfaen County Borough Council e.g. HWB, EDU and Torfaen email accounts are encrypted and secure. Information that is passed to other councils or organisations should be password protected or sent via One Drive where a secure link is generated.
- Check email addresses are correct and avoid autofill especially if responding to a confidential or sensitive email
- Ensure data is minimised when sending emails, a good practice is to reply only to the relevant individual/s. Avoid using 'reply all' unless everyone needs to be included.
- Faxing is to be avoided especially when sharing personal data, if there is no other means of communication then call the recipient and ensure some measures are in place for the person to collect the information prior to sending and follow up to ensure the information has been received.

Storage of data:
- Electronic and paper storage will be held securely
- The School should enforce a clear desk policy
- Paper files that cannot be destroyed are held securely in archive facilities, those that can be destroyed will be done so securely and managed through the appropriate procedures.

Security Breaches:
- The School must manage the security of its information and must make every effort to avoid security and data breaches.
- The School will record all breaches of personal data through the Head teacher and Data Protection and Information Governance Team.
- All staff should be aware of the security breaches procedure (available from the Head teacher/Bursar) and advise their Head teacher and the Data Protection & Information Governance team within 24 hours or without undue delay upon awareness of a breach.
- The School will also monitor information security breaches and will adhere to guidance laid down by the Information Commissioner.

Information Access Controls:
- The School has processes in place to ensure access to information is managed via the User Access Forms, which are completed by Head teachers/Bursars and managed through the SRS.
- The School adopts security controls throughout its buildings to ensure only the appropriate personnel have access to buildings and School equipment. All staff must not allow access to unauthorised personnel, should check identification (and not allow 'tailgating'.)
- The School also undertakes monitoring of IT systems and has an Acceptable Use Policy to ensure that staff are aware of their responsibilities, as well as a Password Policy to comply with information security.

The following individuals/groups have specific responsibilities:

Senior Information Risk Owner (SIRO)	Overall executive responsibility for the Information Security policy and standards and their application throughout the Council The SIRO will work with the Shared Resource Service and the CISO (Chief Information Security Officer) to ensure data and information is protected and will be advised of significant information security breaches
Data Protection Officer	To monitor and promote compliance of the Information Security policy and report back to the service areas via Leadership Team and the IMG The Data Protection & Information Governance Manager will work with the Shared Resource Service and the CISO (Chief Information Security Officer) to ensure data and information is protected and will be advised of IT security breaches from the SRS. Review, implementation, and governance through the Information Asset Owner's Group (IAOG) and Information Management Group (IMG)
Data Protection and Information Governance Team	Policy formulation and review and providing Information Security advice and guidance Ensuring that the Information Security policy (and any related procedures and standards) are kept up to date and relevant to the needs and obligations of the Council
Chief Information Security Officer CISO	Ensuring the security and safety of our systems and infrastructure and reporting any breaches to the SIRO. Can be contacted via security@torfaen.gov.uk
Governors/Head Teachers/Business Managers	Ensuring that these Policies & Procedural documents are made known to all staff, inclusive of agency workers, contractors, volunteers, students or anyone accessing the Council's systems or information and in doing so ensuring awareness of their responsibilities for Information Security To assign clear responsibility for information which passes out of their control following (for example) restructuring, moving of functions, closing of projects
Project Managers/Administrators	To follow the relevant process for Project or Software Approval and where identified, complete Data Protection Impact Assessments (DPIAs) with assistance from the Data Protection & Information Governance team
All staff and Governors	To read and adhere to the Information Security Policy and related procedures/guidance when managing, storing and disposing of the information they create and receive during the course of their duties To undertake any training/awareness provided and understand their responsibilities as employees of the Council To ensure that the information held by the Council is disposed of appropriately and that all sensitive information is disposed of securely To report immediately any observed or suspected incidents where sensitive information has or may have been insecurely disposed of Documenting of processes and evaluating procedures within their service areas
Systems Administrators	Management of the data systems in their service area in conjunction with SRS technical staff. System-specific procedures should be made available to all staff using specialised service area systems such as (but not limited to) Sims/Schools Coms/Class Charts

Shared Resource Service (SRS)	Managing the network infrastructure, ensuring system continuity and security using tools such as encryption, ransomware and regular pen testing
Business Manager	Off-site Archive facility is managed by the Facilities Management Team
Gwent Archives	Gwent Archives is the Accredited Archive Service responsible for selecting, maintaining and archiving records for permanent preservation according to its Appraisal Policy, Archives Collections Policy. HYPERLINK "http://www.gwentarchives.gov.uk/media/94686/collections-care-and-conservation-policy.pdf"See About us.

6. 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 Computer Misuse Act (1990) / (2011)
- 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 Framework
- IG002 Information Governance Policy
- IG006 Acceptable Use Policy
- IG017 Information Sharing Policy
- IG013 Records Management Policy
- IG020 Retention Policy
- IG022 Information Secure Destruction Policy
- IG010 Information Access Policy
- IG012 Information/Data Loss Policy
- IG021 Requests for Information Policy
- IG011 Clear Desk Policy
- IG016 FOI Policy
- IG008 Password Policy
- IG023 BYOD Policy
- IG009 Social Media Policy
- Dignity at Work Policy
- IG101 Offsite Archive & Retention Policy
- IG025 Email 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
- Social Media Guidance
- Code of Conduct for Employees
- IG025 (A) Email Procedures

7.   MONITORING AND REVIEW

The Information Management Groups are responsible for reviewing the content and ensuring that policies are published on the Information Management site on SWOOP. 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.
- An initial 1 year review from policy implementation and on a 3 yearly basis from the current version approval date.

COMPLIANCE

Failure to comply with this policy may be regarded as misconduct and investigated under the Schools' Disciplinary Rules and Procedures. In serious cases this may be considered gross misconduct and lead to dismissal from the School's employment without notice or payment in lieu of notice. In serious cases individuals may be liable for prosecution under Data Protection Law

APPENDIX 1

Terminology	Definition (ISO standards)
Access control	means to ensure that physical and logical access to assets is authorized and restricted based on business and information security requirements
Asset	anything that has value to the organization
Attack	successful or unsuccessful unauthorized attempt to destroy, alter, disable, gain access to an asset or any attempt to expose, steal, or make unauthorized use of an asset
Authenticity	property that is what it claims to be
Confidential information	information that is not intended to be made available or disclosed to unauthorized individuals
Control	measure that maintains and/or modifies risk
Data Protection Impact Assessment (DPIA)	A process to identify and evaluate the risks of processing personally identifiable information (PII) framed within an organization's broader risk management framework
Disruption	incident, whether anticipated or unanticipated, that causes an unplanned, negative deviation from the expected delivery of products and services according to an organization's objectives
Endpoint device	network connected information and communication technology (ICT) hardware device
Information security breach	compromise of information security that leads to the undesired destruction, loss, alteration, disclosure of, or access to, protected information transmitted, stored or otherwise processed
Information security event	occurrence indicating a failure of controls
Information security incident	one or multiple related and identified information security events that can harm an organization's assets or compromise its operations
Information security incident management	exercise of a consistent and effective approach to the handling of information security incidents
Information system	set of applications, services, information technology assets or other information-handling components
Personally Identifiable Information PII	any information that (a) can be used to establish a link between the information and the natural

16

	person to whom such information relates, or (b) is or can be directly or indirectly linked to a natural person
Data Subject	A 'natural' person to whom the personally identifiable information (PII) relates
Processor	that processes personally identifiable information (PII) on behalf of and in accordance with the instructions of a PII controller
Policy	intentions and direction of an organization, as formally expressed by its top management
Procedure	specified way to carry out an activity or a process
Process	set of interrelated or interacting activities that uses or transforms inputs to deliver a result
Record	information created, received and maintained as evidence and as an asset by an organization or person, in pursuit of legal obligations or in the transaction of business
Reliability	property of consistent intended behaviour and results
Sensitive information	information that needs to be protected from unavailability, unauthorized access, modification or public disclosure because of potential adverse effects on an individual, organization, national security or public safety
Threat	potential cause of an unwanted incident, which can result in harm to a system or organization
User	with access to the organization's information systems
Vulnerability	weakness of an asset or control that can be exploited by one or more threats

	from the expected delivery of products and services according to an organization's objectives
Endpoint device	network connected information and communication technology (ICT) hardware device
Information security breach	compromise of information security that leads to the undesired destruction, loss, alteration, disclosure of, or access to, protected information transmitted, stored or otherwise processed
Information security event	occurrence indicating a failure of controls
Information security incident	one or multiple related and identified information security events that can harm an organization's assets or compromise its operations
Information security incident management	exercise of a consistent and effective approach to the handling of information security incidents
Information system	set of applications, services, information technology assets or other information-handling components
Personally Identifiable Information PII	any information that (a) can be used to establish a link between the information and the natural person to whom such information relates, or (b) is or can be directly or indirectly linked to a natural person
Data Subject	A 'natural' person to whom the personally identifiable information (PII) relates
Processor	that processes personally identifiable information (PII) on behalf of and in accordance with the instructions of a PII controller
Policy	intentions and direction of an organization, as formally expressed by its top management
Procedure	specified way to carry out an activity or a process
Process	set of interrelated or interacting activities that uses or transforms inputs to deliver a result
Record	information created, received and maintained as evidence and as an asset by an organization or person, in pursuit of legal obligations or in the transaction of business
Reliability	property of consistent intended behaviour and results
Sensitive information	information that needs to be protected from unavailability, unauthorized access, modification

	or public disclosure because of potential adverse effects on an individual, organization, national security or public safety
Threat	potential cause of an unwanted incident, which can result in harm to a system or or-
User	with access to the organization's information systems
Vulnerability	weakness of an asset or control that can be exploited by one or more threats