William Torbitt Primary School

Information Security Policy

Policy Review

This policy was reviewed and adopted at the Governing Body Meeting in September 2019

This policy is due for review in June 2021

Information security policy

Contents

1 Introduction

Information stored and processed by the school or by third parties working on behalf of the school is a valuable asset. Without adequate levels of protection, confidentiality, integrity and availability of information, the school will not be able to fulfil its obligations including the provision of government services and meeting legal, statutory and contractual requirements.

The school's information is in many forms including:

• Hardcopy documents on paper and sent by fax

• Electronic information stored on computers, remote servers, mobile devices, tapes, microfilm, CDs, external disks and USB portable storage devices

• Verbal information (face to face conversations and over the telephone)

The school are committed to preserving the confidentiality, integrity and availability of the information assets within the jurisdiction of the School for the purposes of:

• sound decision making

• delivering quality services to our customers

• compliance with the law

• meeting the expectations of our customers and citizens

• protecting our reputation as a professional and trustworthy organisation

• safeguarding against fraudulent activity.

This policy sets out the school's commitment to information security and provides the guidelines and frameworks for ensuring all forms of information, supporting systems and networks are protected from security threats such as malicious software, unauthorised access, computer misuse, information technology failures, human error and physical security threats.

The ICT Desk has overall responsibility for the security of Information Assets within the jurisdiction of the school, but it is the responsibility of **all** employees and agents of the school to comply with this policy.

2 Purpose

The purpose of this policy is to protect all information assets within the control of the School from all threats whether internal or external, deliberate or accidental. The policy sets out the controls and requirements that will protect a wide range of information that is generated, shared, maintained and ultimately destroyed or archived.

The purpose of security in an information system or process is to preserve an appropriate level of:

• **Confidentiality:** to prevent unauthorised disclosure of information

• **Integrity**: to prevent the unauthorised amendment or deletion and maintain integrity of information

• **Availability**: to prevent unauthorised withholding of information or resources and ensure information is available as and when legitimately required

• **Resilience**: to ensure that information is accessible when it is needed

3 Scope

This policy applies to all information assets held by the school irrespective of their format and covers all locations into which William Torbitt Primary School information is taken and/or accessed from.

4 Legal Framework

The school must comply with all relevant statutory UK and European Union legislation, including:

- Human Rights Act 1998
- Data Protection Act 2018
- General Data Protection Regulations 2016 (GDPR 2016)
- Freedom Information Act 2000
- Common law duty of confidence
- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990
- Environmental Information Regulations 2004
- Regulation of Investigatory Powers Act 2000
- Health & Social Care Act 2012
- Health and Safety at Work Act 1974
- Telecommunications (Lawful Business Practice) Regulations 2000
- Protection of Freedoms Act 2012
- Waste Electrical and Electronic Equipment (WEEE) Directive
- Re-use of Public Sector Information Regulations 2005

The requirement to comply with this legislation extends to everyone who can be held personally accountable for any breaches of information security for which the School is responsible.

5 Home working/Remote/ Mobile working

All home working and remote/mobile working must be carried out in compliance with the Acceptable Use Policy.

All users working off of the School's site **must** sign the mobile working confidentiality statement (See appendix A) prior to being given access to the network using a virtual private network or virtual machine accessed from non-school equipment

Line Managers are responsible for ensuring that the Mobile Working Confidentiality Statement has been signed when granting permission for remote working.

As part of the issue of laptops or hybrid tablets IT will ensure that staff have signed the mobile working confidentiality statement.

6 Procurement of services

When procuring services all users must ensure that:

• GDPR and Information Governance requirements are clearly specified within the conditions of contract and service specification for all relevant procured services.

• Privacy by Design and Default is mandated and incorporated across all stages of the life cycle development of the service. This mandates the completion of a Data Protection Impact Assessment from the onset for any service provision.

• the school's conditions of contract relating to General Data Protection regulation, freedom of information etc. are included in all relevant procurement information.

• the pre-qualification/evaluation of prospective suppliers includes where appropriate consideration of capability for providing sufficient guarantees with compliance with GDPR.

• due regard is given to GDPR as part of contract monitoring and management.

• the implications of sub-contracting are considered and ensure that the above requirements are passed through the relevant supply chain, with specific considerations for the mandates of the GDPR

• third parties have adequate and demonstrable controls in place with regards to offsite/ remote storage of school information.

7 Disposals

Users must ensure compliance with the Waste Electrical and Electronic Equipment (WEEE) Directive and ensure that sensitive data is not accidentally released. The disposal of any IT equipment **must** be carried out by the IT Unit.

When disposing of any personal, sensitive and/or confidential information staff must do so in accordance with the school's confidential waste disposal procedures.

If working at home staff must comply with the above disposal methods which ensure secure methods such as cross-cut shredding. If no secure disposals methods are available, sensitive information must be transported to your normal working area for secure disposal.

It is important to keep the waste in a secure place until it can be collected for secure disposal. **Never put sensitive and confidential waste in any normal waste bins.**

8 Systems and Software

All information systems which are to be used for storing and processing school information must be formally authorised by the ICT Unit.

Information Asset Owners (IAOs) are responsible for ensuring that Data Protection Impact Assessments are completed for all new systems and information handling processes. They must also ensure that all new systems comply with the Privacy by Design and Default mandate.

User access to systems must be adequately controlled using complex passwords and appropriate access rights. User access rights must be regularly reviewed to ensure they are still appropriate.

Deliberate unauthorised access to, copying, alteration or interference with computer programs or data is strictly forbidden.

User Responsibilities

All persons with IT access (users) **must** undergo the council's Information Security and Data Protection elearning packages.

Users must use a unique username and password for accessing the school's network and information systems.

Users are responsible for keeping their passwords confidential at all times, and must not disclose passwords to anyone, including their line managers. Written down passwords are not permitted Weak passwords must not be used.

Users must not attempt to access systems or records within systems which they have not been formally authorised to access.

Users must not bypass, disable or subvert system security controls.

Users shall ensure that unauthorised persons are not able to view school information on portable devices and shall protect access by locking computers when unattended. This Policy also applies to staff accessing school information on their own devices.

Users must ensure they do not leave portable media such as CDs that contains personal or sensitive information in drives.

All users must inform their manager if they detect, suspect or witness an incident which may be a breach of security and notify the IT Service Desk through the Information Security Breach Guidance.

All users must be aware that the network is monitored. IT Unit will monitor day to day access to ensure adequate protection against security threats, and where necessary, will collect evidence of misuse and unauthorised activity.

Manager's Responsibilities

Managers shall ensure that the School's elearning packages or briefings for Information Security and Data Protection are part of a new employees' induction.

Managers shall ensure that all users complete refresher training for Information Security and Data Protection.

Managers must ensure that when any staff member leaves the School, all school equipment (including their ID card) is returned. The IT Unit must be informed of all leavers immediately to ensure network access is revoked.

Portable hardware including laptops, mobile devices & tablets

Unauthorised equipment must not be connected to the school's network. The exception being personal devices connecting to the school's 'guest' wireless system.

Equipment taken off site must be locked away and kept out of sight when left unattended.
USB ports are restricted and only permit the use of IT approved and encrypted devices. Active scanning will automatically check all media plugged into USB ports to ensure compliance with USB port restrictions.

Equipment left on site overnight e.g. laptops or tablets should be securely stored in a locker or locked cupboard.

9 Information Handling

Building Security

All facilities that hold or process information must have suitable physical security. This includes, but is not limited to:

• **ALL** staff, contractors, agency workers or other persons having access to the School's information assets must wear their ID badge clearly displayed at all times whilst on School premises

• Visitors to office facilities must be escorted at all times while in data processing

• Visitor reception and pass procedures must be followed

• Computer Data Centres will have controlled access and logs recording access

• IT communications equipment must be enclosed in secure locked cabinets if in general office areas

Everyone must ensure that information is not put at risk of damage or theft, and is stored securely and access allowed only to those who need it for legitimate purposes and in accordance with the General Data Protection Regulation For example; Records must be stored in secure buildings with access controls to the building, specific floors and individual offices.

The location of any stored records must be sited to avoid unauthorised access, damage, theft and interference. Stored records must not be removed or moved to another location without notification being given to the relevant Information Asset Owner or Records Co-ordinator.

Electronic information needs to be stored on the school network unless alternative storage (e.g. Cloud) is authorised by the IT Unit.

Users shall not under any circumstances download or store sensitive Council Information (including sensitive personal and personal data) on any non-Council device or facility (e.g. personal cloud).

Communication

Extra care must be taken when printing sensitive information or sending/receiving faxes. When sending sensitive information, a test fax must be sent prior to sending the information or phone the organisation first to let them know what is being sent.

Voicemail may contain personal and sensitive information and therefore passwords must be kept secure

Records Management

Records are a key resource for the effective operation and accountability of the school. It is also recognised that some records will over time become of historical value and need to be identified and preserved accordingly. The Records Management Policy gives more detail about the Council's approach to records management

Removable media

To prevent data loss, the use of USB devices (e.g. portable hard drives, memory sticks) and removable media (e.g. CDs, DVDs, memory sticks etc.) on the council's PCs **must not** be used to store personal and sensitive information unless there is a business requirement to do so.
Users must only use mobile media to transfer personal and sensitive council information if there is a business requirement to do so and there is no other more secure means available e.g. Egress

Only media purchased through the council's IT service and with a sufficient level of encryption, may be used to temporarily hold and transfer personal and sensitive Council information.

10 Information Sharing

Information shall only be shared within the School and with other organisations in line with the law, where there is a need or obligation to do so, and where possible consent has been given.

Where there is a need to enable service delivery through partnership with external organisations the information sharing will be governed either under the terms of a contract or an information sharing or information access /disclosure agreement.

11 Information Security Incidents

Any loss or risk of loss of sensitive and confidential information, either actual or suspected, must be reported immediately without undue delay (within 48 hours of becoming aware of the incident), to the IT Service Desk and notify the Information Governance Lead using the Information Security Breach Guidance.

12 Record of Processing Activities (ROPA))

A Record of Processing Activities will be maintained by Information Asset Owners (and managers) of all the Council's major information assets, including those required for the Council to meet its statutory obligations. Oversight and moderation of the Record of Processing Activities will be provided by the Information Governance Lead.

Appendix A Mobile Working confidentiality statement

Name:

Department:

Address:

I understand that in the course of my duties I may have access to personal and other confidential information relating to residents, clients, colleagues and the Council's partners and contractors. When I am working outside the office environment I understand that I need to take extra care of that information.

I undertake to make sure that any equipment or documentation that I have is secured (preferably in a locked cupboard) when it is in my home and not in use.

I undertake to make sure that any equipment or documentation is not left in my car (or other vehicle, including vehicles belonging to LBR) overnight, and during the day is securely locked in the boot or other secure space where it is concealed.

I undertake to make sure that any information that I have access to, is not exposed to people who do not need to see it, including my family, friends and other visitors to my home. I further undertake to make sure that if I am working in a client's home or a public place that any information that I am using is not exposed to people who do not need to see it.

I undertake to report any breaches of information immediately using the Information Security Incident notification form available on the intranet.

Employee Statement

I also acknowledge that if I breach this confidentiality, I may be liable for formal disciplinary action taken against me. I acknowledge that in addition, I may be subject to criminal prosecution under either the Data Protection Act or Computer Misuse Act or a civil prosecution for damages by the supplier of the information.

Agency Worker / Consultant/ Contractor Statement

I also acknowledge that if I breach this confidentiality, I may be liable for a claim against my professional indemnity and termination of my contract. I acknowledge that in addition, I may be subject to criminal prosecution under either the Data Protection Act or Computer Misuse Act or a civil prosecution for damages by the supplier of the information.

DECLARATION

I, _____

(Name in block capitals)
confirm that I have read the above confidentiality statement, understand it, and agree to abide by it.

_____ _____

Employee / Agency Worker/ Consultant/ Contra... Manager