William Cassidi Church of England Primary School

Cybersecurity Policy Statement

'Life in all Fullness'
(John 10:10)

As a school, we want to provide children with the very best education. To let them experience life in all its fullness and living with all their heart. Our main core value of love underpins all that we do. Our school is Christ-centred and our core Christian values of love, respect, courage, service and resilience flow through every aspect of school life. It is on this bedrock that we provide an excellent education for the children who attend our school. We want every child to be the very best that they can be and to recognise that they are precious, loved and valued.

Policy Statement

An increasing number of schools and colleagues are being seriously impacted by cyber incidents: from phishing attempts to ransomware attacks. As a school we are vigilant in keep the data we hold safe and confidential.

William Cassidi C of E Primary School will ensure the highest level of protection of all information assets within the custody of the school.

High standards of confidentiality, quality and availability of information will be maintained at all times.

William Cassidi will demonstrate support for, and commitment to, information and cyber security through the issue and maintenance of an information and cyber security policy within the school including the supporting guidance documents which are listed below.

Purpose

Every school needs to look after its data as well as manage the risks of using networked computers and services. Information is a major asset that the school has a responsibility and requirement to protect. The secure running of the school is dependent on information being held safely and securely.

Cybersecurity is about protecting the devices we all use and the services we access online – from theft or damage. It is also about preventing unauthorised access to the vast amounts of personal information we store on our devices or in the cloud.

Protecting personal information is a legal requirement under Data Protection Law (GDPR).

The school must ensure that it can provide appropriate assurances to its pupils, parents and staff about the way that it looks after information ensuring that their privacy is protected and their personal information is handled professionally.

Protecting information assets is not simply limited to covering the information (electronic data or paper records) that the school maintains. It also addresses who has access to that information, the processes they follow and the physical computer equipment used to access them.

This Information Security Policy and associated guidance documents, as listed below, address all of these areas to ensure that high confidentiality, quality and availability standards of information are maintained.

The following policy details the basic requirements and responsibilities for the proper management of information assets.

Scope

This Information Security Policy and associated guidance documents, as listed below, apply to all systems, people and school processes that make up the school's information systems. This includes all Governors, school staff and agents of the school who have access to Information Systems or information used for school purposes.

Definition

This policy should be applied whenever school information systems or information is used.

Information can take many forms and includes, but is not limited to, the following:

- Hard copy data printed or written on paper.
- Data stored electronically (on site, on a network or in the cloud).
- Communications sent by post / courier or using electronic means.
- Stored tape or video.

Risks

The school recognises that there are risks associated with users accessing and handling information in order to conduct official school business:

The school is committed to maintaining and improving information security and minimising its exposure to risks.

- Information will be protected against unauthorised access and disclosure.

- The confidentiality of information will be assured.
- The integrity and quality of information will be maintained.
- Authorised staff, when required, will have access to relevant school systems and information.
- Access to information and information processing facilities by third parties will be strictly controlled.
- All breaches of information and cyber security, actual and suspected, will be reported and investigated.
- Information security training will be available to all staff.
- Annual review of Information and Cybersecurity Policy and associated guidance documents, as listed below, will be carried out.
- This policy will be reviewed when significant changes, affecting the school are introduced.
- An Information Security framework of policies and guidance will be developed and implemented consistent with this policy.

Roles and Responsibilities

It is the responsibility of each member of staff to adhere to this policy, standards and procedures. It is the school's responsibility to ensure the security of their information, ICT assets and data. All members of the school community have a role to play in information security.

Staff receive appropriate training and guidance to promote the proper use of information and ICT systems. Staff will also be given adequate information on the policies, procedures and facilities to help safeguard the school's information.

Guidance relating to information security and the use of particular facilities and techniques to protect systems and information, will be disseminated to staff.

Staff are made aware of the value and importance of school information particularly information of a confidential or sensitive nature, and their personal responsibilities for information security. Access to school accounts are maintained via secure passwords that are changed each half term. Information provided to the staff on how to maintain secure passwords. Accounts are not to be shared and accounts locked when not in use.

Two factor authentications provided on sensitive accounts managed by headteacher, ICT Coordinator and OneIT.

All systems (included those to be used outside school) to be protected by Smoothwall firewall maintained by OneIT, in order to protect all users (staff and pupils) from malicious malware or sensitive content.

The practical aspects of ICT protection are performed, such as: keeping all software up to date to ensure they are running latest security patches; maintaining the integrity of the data, producing the requisite back-up copies of data and protecting the physical access to systems and data.

There are appropriate controls over access to ICT equipment and systems and their use including defining and recording the requisite level of protection.

They are the official point of contact for ICT or information security issues and as such have responsibility for notifying the Data Controller (Head Teacher) and the Data Protection Officer (Chair of Governors) of any suspected or actual breach occurring within the school.

Supporting Guidance Documents

The following guidance documents are directly relevant to this policy.

- Internet acceptable use policy
- E-Safety Policy for Schools
- The General Data Protection Register Policy
- Homeworking Guidance
- Information Asset Registers

Policy approved by the Governing Body: December 2024

Date for review: December 2025