Lowton
Church of England High School

Information Security Policy

Original Policy Date:	**December 2018**
Date Reviewed:	**December 2023**
Date of next review:	**December 2026**
Name of Responsible Person:	**Mr D Rostron**

The Governors and staff of Lowton Church of England High School are committed to the provision of a high quality education in a Christian context. We aim to provide a school where we can live out our ethos of Caring, Learning and Succeeding on a daily basis. At the heart of the commitment is the notion of the uniqueness and infinite worth of the individual, that every person is valuable in the eyes of God

This policy has been produced in accordance with the Equality Act 2010 and the Special Education Needs Disability Act 2001, the SEND Code of Practice 2014 and the Children and Families Act 2014. It has been reviewed in accordance with all other school policies and related Acts.

Signed:

Date:

The General Data Protection Regulation (UK GDPR) aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The school is dedicated to ensure the security of all information that it holds and implements the highest standards of information security in order to achieve this. This document sets out the measures taken by the school to achieve this, including to:

- To protect against potential breaches of confidentiality;
- To ensure that all information assets and IT facilities are protected against damage, loss or misuse;
- To support our Data Protection Policy in ensuring all staff are aware of and comply with UK law and our own procedures applying to the processing of data; and
- To increase awareness and understanding at the school of the requirements of information security and the responsibility of staff to protect the confidentiality and integrity of the information that they handle.

Introduction

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

Staff are referred to the school's Data Protection Policy, Data Breach Policy and Electronic Information and Communication Systems Policy for further information. These policies are also designed to protect personal data and can be found on the staff shared drive (N:\Data Protection –GDPR)

For the avoidance of doubt, the term 'mobile devices' used in this policy refers to any removable media or mobile device that can store data. This includes, but is not limited to laptops, tablets, digital cameras, memory sticks and smartphones.

Scope

The information covered by this policy includes all written, spoken and electronic information held, used or transmitted by or on behalf of the school, in whatever media. This includes information held on computer systems, paper records, hand-held devices, and information transmitted orally.

This policy applies to all members of staff including temporary workers, other contractors, volunteers, interns, governors and any and all third parties authorised to use the IT systems.

All members of staff are required to familiarise themselves with its content and to comply with the provisions contained within it. Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the school's Disciplinary Policy and

Procedure up to and including summary dismissal depending on the seriousness of the breach.

This policy does not form part of any individual's terms and conditions of employment with the school and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

General Principles

All data stored on our IT systems are to be classified appropriately (including, but not limited to personal data, sensitive personal data and confidential information. Further details on the categories of data can be found in the school's Data Protection Policy and Record of Processing Activities). All data so classified must be handled appropriately in accordance with its classification.

Staff should discuss with their line manager the appropriate security arrangements for the type of information they access in the course of their work.

All data stored within 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.

All IT Systems are to be installed, maintained, serviced, repaired, and upgraded by IT Support Team or by such third party/parties as the Headteacher may authorise.

The responsibility for the security and integrity of all IT Systems and the data stored thereon (including, but not limited to, the security, integrity, and confidentiality of that data) lies with Network Manager unless expressly stated otherwise.

All staff have an obligation to report actual and potential data protection compliance failures to Headteacher who shall investigate the breach. Any breach which is either known or suspected to involve personal data or sensitive personal data shall be reported to the Data Protection Officer

Physical security and procedures

Paper records and documents containing personal information, sensitive personal information, and confidential information shall be positioned in a way to avoid them being viewed by people passing by as far as possible, e.g. through windows. At the end of the working day, or when you leave your desk unoccupied, all paper documents shall be securely locked away to avoid unauthorised access.

Available locked cabinets, storage rooms and other storage systems with locks shall be used to store paper records when not in use. If you do not feel you have appropriate and/or sufficient storage available to you, you must inform the Caretaking Team as soon as possible.

Paper documents containing confidential personal information should not be left on office and classroom desks, on staffroom tables, or pinned to noticeboards where there is general access unless there is legal reason to do so and/or relevant consents have been obtained. You should take particular care if documents have to be taken out of school.

The physical security of buildings and storage systems shall be reviewed on a regular basis. If you find the security to be insufficient, you must inform the Caretaking Team as soon as

possible. Increased risks of vandalism and or burglary shall be taken into account when assessing the level of security required.

The following measures are taken by the school to ensue physical security of the buildings and storage systems:

- The school carry out regular checks of the buildings and storage systems to ensure they are maintained to a high standard.
- The school has a CCTV system and some areas have fob access systems to minimise the risk of unauthorised people from entering the school premises.
- The school close the school gates during school hours to prevent unauthorised access to the building. An alarm system is set nightly.
- CCTV Cameras are in use at the school and monitored by the Senior Caretaker.
- Visitors should be required to sign in at the reception, accompanied at all times by a member of staff and never be left alone in areas where they could have access to confidential information.

Computers and IT

Responsibilities of the Network Manager

The Network Manager shall be responsible for the following:

a) ensuring that all IT Systems are assessed and deemed suitable for compliance with the school's security requirements;
b) ensuring that IT Security standards within the school are effectively implemented and regularly reviewed, working in consultation with the school's management, and reporting the outcome of such reviews to the school's management;
c) ensuring that all members of staff are kept aware of this policy and of all related legislation, regulations, and other relevant rules whether now or in the future in force, including, but not limited to, the UK GDPR and the Computer Misuse Act 1990.

Furthermore, the Network Manager shall be responsible for the following:

a) assisting all members of staff in understanding and complying with this policy;
b) providing all members of staff with appropriate support and training in IT Security matters and use of IT Systems;
c) ensuring that all members of staff are granted levels of access to IT Systems that are appropriate for each member, taking into account their job role, responsibilities, and any special security requirements;
d) receiving and handling all reports relating to IT Security matters and taking appropriate action in response including, in the event that any reports relate to personal data, informing the Data Protection Officer;
e) taking proactive action, where possible, to establish and implement IT security procedures and raise awareness among members of staff;
f) monitoring all IT security within the school and taking all necessary action to implement this policy and any changes made to this policy in the future; and
g) ensuring that regular backups are taken of all data stored within the IT Systems at regular intervals and that such backups are stored at a suitable location offsite.

Responsibilities – Members of staff

All members of staff must comply with all relevant parts of this policy at all times when using the IT Systems.

Computers and other electronic devices should be locked when not in use to minimise the accidental loss or disclosure.

You must immediately inform the IT Support team of any and all security concerns relating to the IT Systems which could or has led to a data breach as set out in the Breach Breach Policy.

Any other technical problems (including, but not limited to, hardware failures and software errors) which may occur on the IT Systems shall be reported to the IT Support team immediately.

The facility for staff to install software has been disabled. If you wish to install any software onto the network, please contact the IT Support team who will obtain the relevant permissions, licences and undertake the security checks before installing the software.

Software will only be installed where that installation poses no security risk to the IT Systems and where the installation would not breach any licence agreements to which that software may be subject.

The unrestricted USB port has been disabled on all school computers and laptops. Encrypted UBS memory sticks are available from the IT Support team.

If you detect any virus this must be reported immediately to the IT Support team (this rule shall apply even where the anti-virus software automatically fixes the problem).

Access security

All members of staff are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this policy.

The school has a secure firewall and anti-virus software in place. These prevent individuals from unauthorised access and to protect the school's network. The school also teach individuals and students about e-safety to ensure everyone is aware of how to protect the school's network and themselves.

All IT Systems (in particular mobile devices) shall be protected with a secure password, or such other form of secure log-in system as approved by the IT Department.

All passwords must, where the software, computer, or device allows:

a) be at least 6 characters long including both numbers and letters;
b) be changed on a regular basis [and at least every 90 days];
c) cannot be the same as the previous 12 passwords you have used;
d) not be obvious or easily guessed (e.g. birthdays or other memorable dates) and meet the minimum password complexity requirements (6 characters, 1 capital and 1 number)
e)

Passwords must be kept confidential and must not be made available to anyone else unless authorised by a member of the Senior Leadership Group who will liaise with the IT Support

team as appropriate and necessary. Any member of staff who discloses his or her password to another employee in the absence of express authorisation will be liable to disciplinary action under the school's Disciplinary Policy and Procedure. Any member of staff who logs on to a computer using another member of staff's password will be liable to disciplinary action up to and including summary dismissal for gross misconduct.

If you forget your password you should notify the IT Support team to have your access to the IT Systems restored. You must set up a new password immediately upon the restoration of access to the IT Systems.

You should not write down passwords if it is possible to remember them. If necessary you may write down passwords provided that you store them securely (e.g. in a locked drawer or in a secure password database). Passwords should never be left on display for others to see.

Computers and other electronical devices with displays and user input devices (e.g. mouse, keyboard, touchscreen etc.) shall be protected with a screen lock that will activate after a period of inactivity. You may not change this this time period or disable the lock.

All mobile devices provided by the school, shall be set to lock, sleep, or similar, after a period of inactivity, requiring a password, passcode, or other form of log-in to unlock, wake or similar. You may not alter this time period.

Staff should be aware that if they fail to log off and leave their terminals unattended they may be held responsible for another user's activities on their terminal in breach of this policy, the school's Data Protection Policy and/or the requirement for confidentiality in respect of certain information.

Data security

Personal data sent over the school network will be encrypted or otherwise secured.

All members of staff are prohibited from downloading, installing or running software from external sources without obtaining prior authorisation from Network Manager who will consider bona fide requests for work purposes. Please note that this includes instant messaging programs, screen savers, photos, video clips, games, music files and opening any documents or communications from unknown origins. Where consent is given all files and data should always be virus checked before they are downloaded onto the school's systems.

You may connect your own devices (including, but not limited to, laptops, tablets, and smartphones) to the school's Wi-Fi provided that you follow the Network Manager requirements and instructions governing this use. All usage of your own device(s) whilst connected to the school's network or any other part of the IT Systems is subject to all relevant school Policies (including, but not limited to, this policy). The Network Manager/IT Support team may at any time request the immediate disconnection of any such devices without notice.

Electronic storage of data

All portable data and in particular personal data should be stored on encrypted drives using methods recommended by the Network Manager.

All data stored electronically on physical media, and in particular personal data, should be stored securely in a locked box, drawer, cabinet, or similar.

You should not store any personal data on any mobile device, whether such device belongs to the school or otherwise without prior written approval of the Network Manager. You should delete data copied onto any of these devices as soon as possible and make sure it is stored on the school's computer network in order for it to be backed up.

All electronic data is backed up to a disk storage unit on a daily basis. Critical data is backed up to the Cloud Disaster Recovery system and is stored offsite in a UK data centre. This system is overseen by the Network Manager.

Home working

You should only take confidential or other information home where appropriate technical and practical measures are in place within your home to maintain the continued security and confidentiality of that information.

You must ensure that:

a) the information is kept in a secure environment; and
b) all confidential material that requires disposal is returned to school and disposed of in the confidential waste bins. See Disposal of Confidential Waste Policy for more information

Communications, Transfer, Internet and Email Use

When using the school's IT Systems you are subject to and must comply with the school's ICT Acceptable Use and Electronic Information and Communication Systems Policies.

The school work to ensure the systems do protect students and staff and are reviewed and improved regularly.

If staff or students discover unsuitable sites or any material which would be unsuitable, this should be reported to Headteacher/Designated Safeguarding Officer and Network Manager.

Regular checks are made to ensure that filtering methods are appropriate, effective and reasonable and that users access only appropriate material as far as possible. This is not always possible to guarantee and the school cannot accept liability for the material accessed or its consequence.

All personal information, and in particular sensitive personal information and confidential information should be encrypted before being sent by email or recorded delivery.

Postal and email addresses and numbers should be checked and verified before you send information to them. In particular you should take extra care with email addresses where auto-complete features may have inserted incorrect addresses.

You should be careful about maintaining confidentiality when speaking in public places.

You should make sure to mark confidential information 'confidential' and circulate this information only to those who need to know the information in the course of their work for the school.

Personal or confidential information should not be removed from the school without prior permission from the Headteacher except where the removal is temporary and necessary e.g. student marking. When such permission is given you must take all reasonable steps to

ensure that the integrity of the information and the confidentiality are maintained. You must ensure that the information is:

a) not transported in see-through or other un-secured bags or cases;
b) not read in public places (e.g. waiting rooms, cafes, trains, etc.); and
c) not left unattended or in any place where it is at risk (e.g. in car boots, cafes, etc.)

Reporting security breaches

All concerns, questions, suspected breaches, or known breaches shall be referred immediately to the Headteacher. All members of staff have an obligation to report actual or potential data protection compliance failures.

When receiving a question or notification of a breach, the Headteacher shall immediately assess the issue, including but not limited to, the level of risk associated with the issue, and shall take all steps necessary to respond to the issue.

Members of staff shall under no circumstances attempt to resolve an IT security breach on their own without first consulting the Headteacher Any attempt to resolve an IT security breach by a member of staff must be under the instruction of, and with the express permission of, the Headteacher

Missing or stolen paper records or mobile devices, computers or physical media containing personal or confidential information should be reported immediately to Headteacher.

All IT security breaches shall be fully documented.

Full details on how to notify of data breaches are set out in the Breach Notification Policy.

Related Policies

Staff should refer to the following policies that are related to this information security policy:

- Acceptable Use Policy
- Electronic Information and Communication Systems Policy
- Data Breach Policy
- Data protection Policy

Date	Description of Change
November 2022	Updated reference to UK GDPR Related policies updated Formatting changes