LITTLE HEATH SCHOOL
ICT ACCEPTABLE USE POLICY

Purpose and background

Little Heath School seeks to embrace the use of ICT to enhance teaching, learning and administration within the school.

To help ensure as far as possible safe and appropriate use of ICT in school and, when related to the work of the school, remotely, it is necessary to outline the principles underpinning appropriate computer use, make expectations clear and ensure users are fully aware of the consequences of not following the protocols that have been laid down and indulging in computer misuse.

The main body of this policy applies to:

- all staff of Little Heath School who may have access to a school owned computer, regardless of whether or not they use it in their day to day work routine;
- all staff of Little Heath School who may use their own privately-owned ICT equipment whilst on the school's premises;
- all staff of Little Heath School who may remotely access the school network;
- all visitors/guests of Little Heath School who may be connecting to the school network either via school equipment or their own personal equipment;
- all third parties or suppliers who may remotely access any school equipment in the course of their work with the school.

Appendix 1 of this policy gives specific guidance regarding acceptable use of ICT in school by pupils.

This acceptable use policy provides guidance on what is appropriate use of ICT within Little Heath School and when working remotely. The policy supplements any legislation around ICT use, such as the Data Protection Act 2018, General Data Protection Regulation (GDPR) 2018, Copyrights, Designs and Patents Act 1988 and the Computer Misuse Act 1990. This policy also supplements government guidelines and initiatives such as the Child Exploitation and Online Protection Body (CEOP).

Policy objectives

This policy aims to:

- enhance teaching and learning, both in school and when working remotely, by the effective use of ICT;

- enable ICT to effectively support the school's administration processes;
- ensure suitable procedures are in place that support effective management of the school's ICT infrastructure and network;
- promote safe use of the internet by staff and pupils;
- help ensure safe and appropriate use of ICT by staff, pupils, contractors and other visitors, both in school and remotely;
- provide suitable and proportionate rights of investigation when there are genuine grounds to suspect a breach of the school's ICT procedures or any ICT related legislation.

Management of policy

School:	This policy is implemented and managed by the School Business Manager, the Assistant Head with responsibility for ICT for Learning, and the Headteacher, in conjunction with the school's IT Managed Service Provider.
Governing Body:	The Governing Body has delegated the oversight, review and updating of this policy to its Finance and Resources Committee.
Approval:	Approved by the Finance and Resources Committee on 1 July 2021.
Next review due:	June 2024

Associated policies

Staff Disciplinary Policy
Display Screen Equipment (DSE) Policy
Data Protection Policy
Freedom of Information Policy
Behaviour Policy
Charging and Remissions Policy
Safeguarding Policy
Press and Media Policy
Complaints Policy

Practice and procedures

Communication of this policy

This ICT Acceptable Use Policy (ICT AUP) is published on the Little Heath School website, together with appendices 1 and 2. A full copy, including all appendices, is available to staff on the school's X Drive and an electronic copy is given to each member of staff when they join the school as part of the induction process. Each new member of staff is required to sign a ICT AUP Agreement form (appendix 10) and return this to the School Business Manager signifying their acceptance of the policy before they can be given an account with access to the network. In signing, they accept that they agree to all future revisions of the policy which will be published on the school's website and X Drive as set out above, unless the Headteacher is notified in writing by the individual.

Staff already employed by the school at the time that this policy was first published were required to sign an ICT AUP Agreement within a period of one month from when the policy was issued electronically to all staff. In signing they accepted that they agreed to all future revisions which will be published on the school's website and X Drive as above, unless the Headteacher is notified in writing by the individual.

When the ICT AUP is updated a new version is provided to all staff electronically and published on the website and X Drive as set out above.

Visitors, guests and suppliers must be advised of the ICT AUP when attending the school if they are going to use ICT whilst on the school premises.

Hard copies of this policy are available on request via the main school office.

Consequences of improper conduct

Failure to abide by this AUP will be treated in the same way as any other misconduct issue, in accordance with the school's Staff Disciplinary Policy. A serious breach could ultimately result in dismissal. Illegal activities will be reported to the police and if necessary the Local Safeguarding Children Authority.

General computer use

In general, use of ICT equipment (such as computers, printers), email and the internet within the school should be primarily to enhance teaching and learning or for school administrative use. It is understood however that users may occasionally need to use ICT for personal reasons and this is permitted as long as such use does not interfere with or lessen their work and does not conflict with other aspects of this policy. Priority for computer usage should always be given to the core functions of the school.

Use for business purposes not related to school activities, or for personal gain, is not permitted.

User accounts

User accounts are the responsibility of the user. Passwords must be kept secure and should be strong ie not easy to guess. Passwords must not be written down or disclosed to anyone.

Users must not allow anyone else to use their account nor should they use anyone else's account.

Staff must log off or lock their account when away from a computer that they are in the process of using. Accounts are not to be left logged in and unattended as it may enable unauthorised access to the user's profile, including their email account.

Some areas of the school (such as the main office and the site team) have a generic email user account, which can be used by a number of individuals. The number of generic accounts will be kept as low as possible and they will only be set up where there is a clear business case to do so. Use of each generic user account must be controlled by one named individual who is responsible for:

- controlling access to that account
- ensuring the password is changed regularly
- maintaining a clear understanding of who is using the account, when and for what purpose. Any changes will need to be made by the school's IT Managed Service with reference to existing authorities.

Hardware and software

All users are responsible for the care and safe-keeping of any ICT equipment. Portable equipment such as laptops and data storage media such as CDs must be kept securely locked away when not in use.

Liquids and food must be kept away from any ICT equipment and staff are made aware of the health and safety hazards relating to electrical equipment.

Software is licensed and must only be installed by the school's IT Managed Service Provider and then only on the machines for which it has been purchased. The IT Managed Service Provider will only install software where specific permission to do so has been given by the Headteacher or School Business Manager.

To comply with the Copyright, Designs and Patents Act 1988:

- users are not permitted to install unlicensed software on any machine

- users are not permitted to copy licensed software for installation on other machines (school or non-school equipment).

Users are not permitted to download and install non-licensed software packages without gaining prior approval from the Headteacher or School Business Manager via the IT Managed Service Provider.

Any ICT hardware or software purchased for school purposes must be ordered via the IT Managed Service Provider. Requests for additional hardware or software, or for equipment to be moved, should be submitted using the form in appendix 6. Such requests will be collated and considered by the school's IT Operations Group on no less than a monthly basis.

Users should report all faults with ICT hardware or software to the IT Service helpdesk, either via phone or email, as soon as they are identified and staff should not attempt to repair ICT equipment themselves.

Disposal of old/broken equipment must be arranged via the IT Managed Service Provider as disposal of electrical equipment is now subject to UK government regulations (Waste Electrical and Electronic Equipment (WEEE) Regulations 2013)

Laptop users

All staff who have a Little Heath School laptop issued to them must sign the Staff Laptop Agreement (see appendix 9).

Data

Data must be kept in accordance with the General Data Protection Regulation 1998. In broad terms, anyone who processes personal information must comply with eight principles, which make sure that personal information is:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than is necessary
- Processed in line with an individual's rights
- Secure
- Not transferred to other countries without adequate protection

Staff must not disclose any information to a third party that could be considered sensitive information. If a member of staff is unsure as to whether information should be released, they should not release it until they have sought appropriate advice.

Staff must not risk accidental disclosure of sensitive information and must therefore abide by the following:

- when leaving a computer unattended it must be locked or the user must have logged out
- passwords must be kept secure and should be changed regularly (at least once every 12 weeks ie every long term)
- passwords must not be written down or disclosed to anyone.
- staff must not allow anyone else to use their account and they must not use anyone else's account

If necessary, sensitive data should be protected with passwords.

Data stored on devices such as CDs, DVDs, data sticks and external hard-drives (i.e. not just on computers/laptops) is also at risk and subject to the General Data Protection Regulation 2018.

Users are responsible for day to day management of their data, being aware of their data storage limits (see appendix 4) and ensuring unwanted material is deleted on a regular basis. Documents which are needed by multiple users should be stored in department areas of the network or on Sharepoint to avoid multiple copies being stored. Little Heath School's file naming protocols are set out in appendix 4.

The school's IT Managed Service Provider should be contacted for advice on how best to store large amounts of data such as photographs and video files.

Personal data, for example photos, should not be stored on the school network.
.

Internet usage

All use of the internet within the school, whether on a personal or school owned device, should be primarily to enhance teaching and learning or for administrative use. It is understood however that users may occasionally need to use the internet for personal reasons but this should not be at the expense of work.

Use of the internet within the school for the conducting of private business or personal gain is not permitted.

Staff are not permitted to use the internet for any illegal activity; although not specifically against the law this includes accessing sites meant for adults of 18 years or older such as pornographic and gambling websites. Staff must not search for, or browse through, any sites that contain offensive, obscene, violent, dangerous or inflammatory material.

The downloading of any unlicensed material such as music, video, TV programmes, games, PDF files is illegal and therefore not permitted.

Email

All users are provided with a @littleheath.org.uk email account for school related use. The email address should not be used for personal emails.

Attachments on emails are currently limited to 25MB (this can be kept under review subject to operational requirements). Anyone needing to send anything over this size should contact the school's IT Managed Service Provider for advice on how to compress larger files.

Users are responsible for day to day management of their emails and ensuring unwanted material is deleted on a regular basis.

Email is treated as data and therefore is subject to the General Data Protection Regulation 2018.

If email is accessed remotely from the school by staff using a personal or public use computer they must:

- not store anything on the computer hard-drive
- if accessing in a public place, be careful no one can see what they are doing
- make sure they log off completely.

Email should be treated as inherently insecure. Staff must not open or forward any email or attachment from an unrecognised source or that they suspect may contain inappropriate material or viruses. They should instead report them to the school's IT Managed Service Provider.

Automatically generated email responses should be used with care. Staff should be cautious about including personal information such as holiday dates and contact numbers.

Protocols for email usage by staff at Little Heath School are set out in appendix 3.

Email and internet filtering and monitoring

The school has in place a sophisticated filtering & monitoring system which:

- checks for viruses and traps suspicious emails
- denies access to most undesirable and inappropriate sites on the Internet
- maintains a list of banned sites which is updated on a regular basis.

Whilst this provides a measure of reassurance it must be understood that the filter does not trap or block everything.

Details of the school's approach to web filtering for different cohorts is set out in appendix 7.

Staff need to be aware that:

- staff emails to and from the school can be monitored for inappropriate use if deemed necessary by the Headteacher
- internet access within the school can and will be monitored for inappropriate use
- all internet sites accessed by users are logged with the date and time of access

Misuse of the internet and/or email will always result in an investigation as detailed under the school's Staff Disciplinary Policy. The accessing and use of inappropriate and indecent materials from the internet or via email will result in disciplinary action being taken, which could lead to dismissal.

Social networking sites

Access to social networking sites using school IT equipment is generally blocked. Limited access to particular sites may however be permitted on request for limited periods and/or for limited groups, if access is required to fulfil a specific teaching and learning purpose linked to curriculum need.

Staff are not permitted to have school students as contacts on social networking sites and are advised to be cautious when allowing contact with other minors (those under 18 years of age) in case of a second or third level connection to a school student. Staff are reminded that ex-pupils may have friends who are still at the school. Privacy settings for personal profiles (and any groups joined) should be used. Staff must never use a personal profile site for school purposes but instead should create a new user profile for this.

Staff should not discuss any school related matters, or identify their place of work, when using public access social networking sites. Care must be taken in order to avoid bringing the school in to disrepute.

The Headteacher reserves the right to request access to social networking sites if an infringement of this policy is suspected.

Further information on use of social media can be found in appendix 12 of this policy.

Bullying/Cyber-bullying/Online Bullying

The school will not tolerate any form of bullying including electronic or online bullying.

The misuse of email systems or the internet for harassing people, such as by sending unpleasant or aggressive messages ('cyber bullying') is on the increase. The proliferation of social networking websites such as Myspace, Bebo and Facebook has made it easier for people to stay in touch with each other but is also being used as a medium to enable harassing and bullying. The school reserves the right to monitor all internet and email activity within the bounds of current legislation in order to keep the internet safe for all at Little Heath School and to protect from online bullies.

Any instances of bullying will be taken very seriously. As with any other form, cyber or online bullying (involving the use of personal computers, mobile phones etc) will be investigated fully and may result in disciplinary action leading to possible dismissal.

Pornography & other inappropriate material

Staff are not permitted to access or save any form of pornography or offensive, obscene, violent, dangerous or inflammatory material onto computers. The Headteacher reserves the right to perform spot checks on accounts and computers at any time when there is believed to be just cause to do so. If any inappropriate material is found, the account will be disabled immediately and disciplinary action procedures will begin, in line with the school's agreed Disciplinary policy.

Hacking

The Computer Misuse Act 1990 makes it illegal to:

- gain unauthorised access to a computer's software or data (hacking), including the illegal copying of programs
- gain unauthorised access to a computer's data with the intent to commit or facilitate further offences
- gain unauthorised access to a computer's data with the intention of altering or deleting it, including planting viruses
- copy programs illegally (software piracy).

Any type of hacking (defined as an attempt to gain access to folders, databases, or other material on the network to which one is not entitled) is considered to be an extremely serious offence. To comply with the Computer Misuse Act 1990 any user who indulges in hacking or is found with hacking software/paraphernalia on their computer or network account is liable to be dismissed. Likewise, physical

interference with another user's computer or school-owned computer will not be tolerated.

Associated documents

Staff Code of Conduct

Appendices

Appendix 1: Code of Practice for Acceptable Use of ICT by Pupils
Appendix 2: Bring Your Own Device – for pupils
Appendix 3: Email Protocols
Appendix 4: Storage of Data
Appendix 5: Remote Access
Appendix 6: Request form: additional hardware, software or equipment moves
Appendix 7: Web Filtering
Appendix 8: Back-Up Procedures
Appendix 9: Staff Laptop Agreement
Appendix 10: Staff ICT Acceptable Use Policy Agreement
Appendix 11: Prevent Statement
Appendix 12: Use of Social Media
Appendix 13: Remote Learning Policy