



# **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. Expectations need to be clear and it must be ensured that users are fully aware of the consequences of not following the protocols that have been laid down or of indulging in computer misuse.

This policy applies to:

- all staff and students of Little Heath School who may have access to a school owned computer on the school premises;
- all staff and students of Little Heath School who may use their own IT equipment whilst on the school premises;
- all staff and students of Little Heath School who may remotely access the school network using their own or a school owned device;
- all visitors to Little Heath School who may be connecting to the school network or wifi, 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.

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 2022. 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 the effective operation and management of the school's ICT infrastructure and network;
- promote safe use of the internet by staff and students;
- help ensure safe and appropriate use of ICT by staff, students, 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 Deputy 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 2024

**Next review due:** June 2027

### **Associated policies**

Staff Disciplinary Policy  
 Data Protection Policy  
 Freedom of Information Policy  
 Behaviour Policy  
 Safeguarding Policy  
 Press and Media Policy  
 Complaints Policy

### **Practice and procedures**

#### Communication of this policy to staff

A full copy of the policy, including all appendices, is available to staff on the school's intranet.

Every new member of staff is required to read a full copy of the policy when they join the school, as part of the first day of their induction process. They are then required to sign an electronic ICT AUP Agreement to signify their acceptance of the policy. Any concerns over signing should be raised with the Headteacher.

Staff already employed by the school at the time of publication of this policy in 2024 are required to sign an electronic ICT AUP Agreement within a period of one month from when the policy was made available on the intranet. Any concerns over signing should be raised with the Headteacher.

When the ICT AUP is updated, staff will be notified and the policy will be published on the intranet.

#### Communication of this policy to students

This policy is published on the Little Heath School website, together with appendix 2 which specifically applies to students. These documents are brought to the attention of every new student, via their parent or carer, as part of the induction process.

The Code of Practice has also been brought to the attention of every existing student, via their parent or carer, at the time that the Code of Practice was first approved by the school governors and published on the school website in 2024.

Any significant updates to the Code of Practice will be brought to the attention of all students via their parent or carer, as well as in school.

#### Communication of this policy to visitors and other third parties

Visitors and other third parties must be advised of the ICT AUP when attending the school, if they are going to use ICT equipment or the school's internet whilst on the school premises, or if they will be accessing the school's IT systems remotely. Personalised guest wifi access codes can be arranged via the school's IT Managed Service.

#### **Associated documents**

Staff Code of Conduct  
Home-School Agreement

#### **Appendices**

Appendix 1: Code of Practice for Acceptable Use of ICT by Staff  
Appendix 2: Code of Practice for Acceptable Use of ICT by Students

## **Appendix 2: Code of Practice for acceptable use of ICT by Little Heath School Students**

Little Heath School seeks to embrace the use of ICT to enhance teaching and learning. Nevertheless, a Code of Practice is needed in order to outline the principles underpinning appropriate computer use, make expectations clear and ensure students are fully aware of the consequences of not following the Code of Practice and indulging in computer misuse.

This Code of Practice supplements any legislation around ICT use such as:

- The General Data Protection Regulation (GDPR) 2018;
- Data Protection Act 2018
- Computer Misuse Act 2022;
- Copyright, Designs and Patent Act 1988;

and government guidelines and initiatives such as the Child Exploitation and Online Protection Body (CEOP).

Students are provided with access to the school network, internet and email system in order to enable them to carry out their school work. Access is however only granted on the understanding that students follow the reasonable guidelines set out below. Students who abuse any rules may face sanctions following an investigation, for example their account may be suspended or deleted. Any illegal activity may be reported to the appropriate authorities.

Students need to be aware that:

- emails to and from the school network can be monitored for inappropriate use;
- internet access within the school can and will be monitored for inappropriate use;
- all internet sites accessed by users are logged with date and time of access;
- the school reserves the right to perform spot checks on accounts and any computer at any time;
- the school reserves the right to delete any data that should not be stored on the school network, without prior reference to the student concerned.

### **Personally-owned equipment**

As well as using school-owned ICT equipment in the course of their academic studies, students of Little Heath School are permitted to use personal ICT equipment, such as laptops and mobile phones, within certain guidelines (which

may vary between different age groups) as long as such use does not interfere with academic activities and does not conflict with other aspects of this Code of Practice. The conditions stated within this Code of Practice apply to both school-owned and personally-owned equipment. At the current time only Sixth Form students are permitted to use their own laptop or tablet devices on the school premises.

The school will not be liable for loss of or damage to any personally-owned equipment and neither the school nor its IT Managed Service Provider are responsible for supporting or repairing any personally-owned machine. 'Damage' extends to include any viruses, malware, spyware etc that may be picked up as a result of connecting to the school's network or internet.

If a student wishes to store school work on their personal computers they should remember to back it up regularly to the school network to prevent accidental loss.

Any software on personally owned machines which are brought in to school, or which are used for school related study, should be legally licensed as software piracy is illegal.

If students bring a mobile phone in to school, they are expected to only use it on school site (either via its data plan or school wifi) in accordance with this Code of Practice and the school's mobile phone policy.

# RESPONSIBLE ICT USE – EXPECTATIONS OF STUDENTS

## LITTLE HEATH SCHOOL



### SECURITY

- Students must only use their own usernames and passwords, and must keep them private.
- School systems must be used responsibly and only for learning purposes.
- Students must log off when they have finished working on a computer.
- Students must only use Little Heath authorised software on school equipment and should not download or install it themselves.
- Students must not use, or attempt to use, any form of proxy or other method to get round the school's web filtering.

### EMAIL, INTERNET, CHAT and FORUMS

- Students must only use their school email account for school related communication, not their own personal accounts.
- Students must write all emails and messages in a careful and polite way to all people.
- Students must not disclose any personal information, or photos/videos about anyone, to another person.
- Students must use the internet responsibly and only with permission from teachers or other school staff. Students must not attempt to search for inappropriate content.
- Students must not access websites or games which are irrelevant to their school work or download unlicensed material.
- Students in Key Stages 3 and 4 must not access social networking sites whilst in school, unless it has been approved in relation to school-owned devices as part of the curriculum.
- Students in Key Stage 5 are permitted to access social networking sites on their personal devices while in school, but only during break and lunchtimes.
- Students must not set up email groups/distribution lists.
- Students must not open or forward an email or attachment from an unrecognized email address or that they suspect may contain inappropriate material or viruses. Such emails must be reported to a teacher.

### SAFETY AND BULLYING

- Students must respect all people when online, whether through email, messaging, social networking or the internet.
- Students must tell their tutor, computing teacher or an appropriate adult if they find anything inappropriate or unsafe whilst online.

- Students must ensure that their use of the school computer systems or websites does not include anything which may offend, hurt or scare people.

### **EQUIPMENT AND FILES**

- Students must take care of all school computer equipment and report any faults to their teacher. Students should not attempt to repair equipment themselves.
- Food and drink must be kept away from ICT equipment.
- Students will be held responsible for any damage that they cause to IT systems through inappropriate behaviour. This includes invoicing a student's parents for the cost of any repairs or replacement that are necessitated by the student's actions.
- Students must keep their emails and data on the school network well organised, regularly deleting items that are no longer needed.
- Students must not store any files which are in breach of copyright law and they must only use the school's systems for information related to their academic studies or recognised extra-curricular school activities.