Appendix 1

CODE OF PRACTICE FOR ACCEPTABLE USE OF ICT BY PUPILS

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 pupils 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 1990;
- Copyright, Designs and Patent Act 1998;
- Health and Safety (Display Screen Equipment) Regulations 1992 (amended 2002);

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

How is this code of practice communicated and updated?

This code of practice is published on the Little Heath School website and is brought to the attention of every new pupil, via their parent or carer, as part of the induction process. The code of practice was also brought to the attention of every existing pupil, via their parent or carer, at the time that the code of practice was first approved by the school governors.

From Academic Year 21/22, responsible use of IT will be incorporated in to the school's Home-School agreement which is signed by parents and students.

Any significant updates to the code of practice will be brought to the attention of all pupils via their parent or carer, as well as in school. Paper copies of this code of practice are available on request from the main school office.

What are the consequences of improper conduct?

Failure of a pupil to abide by this code of practice will be investigated and processed in the same way as any other form of behaviour issue and, ultimately, could result in a fixed term or even permanent exclusion. Improper conduct may also result in pupils losing privileges or their IT account being blocked. Illegal activities will be reported to the Headteacher and if necessary the Local Safeguarding Children Authority and Social Services.

General computer use

As well as using school-owned ICT equipment in the course of their academic studies, pupils 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. Where there is a material difference this is specifically identified.

In general, use of school-owned ICT equipment (such as computers and printers), email and the internet within the school should be primarily to enhance teaching and learning. Priority for computer usage should always be given to the core teaching and learning functions of the school.

Personally-owned equipment

Pupils and parents must be aware of the risks of bringing valuable items into school and it is recommended that parents ensure that their own insurance policies cover this.

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.

.

Pupil accounts

Pupil accounts are allocated when joining the school. Pupil accounts are the responsibility of the pupil and the following should be followed:

- passwords must be kept secure;
- pupils must not write their password down or disclose it to anyone;
- pupils must not allow anyone else to use their account and should not use anyone else's account;
- pupils must log off or lock their account when away from a machine, never leaving their account logged in and unattended.

Hardware and software

All pupils have a responsibility towards the care and safe-keeping of any ICT equipment. Any wilful damage to equipment will be charged to the pupil responsible with an invoice sent home to their parent or carer.

Liquids and food must be kept away from any ICT equipment and pupils must have at least a basic awareness of the health and safety hazards relating to electrical equipment.

Pupils are not permitted to download and install software packages on school-owned equipment and should ensure that any software on personally-owned machines which are brought in to school or used for school related study is legally licensed. Software piracy is illegal.

Pupils should report all faults on school-owned equipment to a member of staff who will contact the school's IT Managed Service Provider as necessary. Under no circumstances should a pupil attempt to repair ICT equipment themselves.

Data

Data must be kept in accordance with the General Data Protection Regulation 2018.Pupils must not disclose any information about someone to another person that could be considered sensitive information. An example of sensitive information would be personal data such as names, addresses, telephone numbers, email addresses etc.

Pupils are responsible for day to day management of their data stored on the pupil network, being aware of the data storage limits (500MB per pupil) and ensuring unwanted material is deleted on a regular basis. Pupils must only store data on the school network that is related to their academic studies or recognised extra-curricular school activities. The school reserves the right to delete data that does not fall within these parameters, without prior reference to the pupil concerned.

Pupils storing data such as course work on personal laptops should remember to back it up regularly to data sticks or CDs/DVDs to prevent accidental loss. The work should also be backed up regularly to the school network.

Internet usage

All use of the internet within school hours should be primarily to enhance teaching and learning. It is understood that pupils may wish to use the internet for personal reasons. This is permitted as long as it does not interfere with academic activities and does not conflict with other aspects of this code of practice.

Pupils are not permitted to use the internet for any illegal activity; this includes accessing sites meant for adults of 18 years or older such as pornographic or gambling sites. Pupils must not search for, or browse through, any sites that contain offensive, obscene, violent, dangerous or inflammatory material.
Use of the school internet and network for the conducting of private business or personal gain is not permitted. The downloading of any unlicensed material such as music, video, TV programs, games, and PDF files is illegal and therefore not permitted.

Any student found to be using any form of proxy or other method to circumvent the school's security software will be subject to the school's disciplinary procedures, even if the site being accessed is harmless in itself.

If students have their own equipment with a data plan, such as a mobile phone, they are expected to only use it on school site in accordance with the school's Acceptable Use Policy, the same as if it was a school owned device.

Email

All pupils are provided with a @littleheath.org.uk email account. Attachments on pupil emails are limited to 25MB.

Pupils are responsible for day to day management of their emails including ensuring unwanted material is deleted on a regular basis. Pupils need to be aware that email is treated as data and therefore is subject to guidelines of the General Data Protection Regulation 2018.

If email is being accessed using a personal or public (rather than a school-owned) computer:

- no information is to be stored on the computer hard-drive;
- if accessing in a public place, pupils need to be aware of who may be watching;
- pupils must ensure they log off completely.

Email should be treated as inherently insecure. Pupils 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 the item to a teacher who will refer the matter to the school's IT Managed Service Provider.

Pupils must not respond to emails that request personal details. In general organisations will not request personal data via email.

Pupils must not send, forward, print or transmit in any form any offensive, obscene, violent, dangerous or inflammatory material via email. As with any form of correspondence pupils are to be aware of the language they use in emails to ensure it is not inappropriate.

Pupils are not permitted to send or forward chain letter emails, jokes, spam etc.

If a pupil is concerned about any email they have received they should contact a member of staff immediately. If a pupil feels they are being bullied via email they should follow the guidance provided later on in this code of practice.

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

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.

Pupils 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.

Misuse of the internet and/or email will always result in an investigation and disciplinary procedures where necessary.

The accessing and use of inappropriate and indecent materials from the internet or via email will result in disciplinary action being taken which could result in a fixed or permanent exclusion.

Social networking sites

Access to social networking sites is not permitted on school-owned devices. The only exception to this will be if selected pupils are granted temporary access in order to be able to meet the requirements of certain academic courses.

Pupils are not permitted to have Little Heath School staff (teaching or non-teaching) as contacts on social networking sites. The Headteacher reserves the right to request access to social networking sites if he suspects an infringement of the school rules or that there is a potential safeguarding issue.
.
Whilst use of social networking sites has brought about a communications revolution that gives young people unrivalled opportunities, it also brings risks.
It is important that pupils understand these risks, know how to stay safe in this environment and how to avoid making themselves vulnerable to a range of issues including identity theft, bullying, harassment, grooming and abuse. They also need to learn how to avoid the risk of exposing themselves to subsequent embarrassment due to an inappropriate personal profile or inclusion on another's profile. The school's website contains up to date information and advice on internet safety, for both pupils and parents.

Bullying, cyber-bullying and online bullying

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

If any pupil feels they are being bullied or harassed they should:

- talk to their form tutor, Head of Year or another member of staff, and/or
- go to the Student Voice Office at break or lunchtime, and/or
- send an email to:smile@littleheath.org.uk.

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 will result in disciplinary action leading to possible exclusion.

Pornography & other inappropriate material

Pupils are not permitted to access or save any form of pornography or offensive, obscene, violent, dangerous or inflammatory material onto any computer. The school reserves the right to perform spot checks on accounts and any computer at any time. If any inappropriate material is found, the account will be disabled immediately and disciplinary action will begin.

Hacking

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 pupil who indulges in hacking or is found with hacking software/paraphernalia on their computer or network account is liable to be excluded.

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