LOUGHBOROUGH
High School

Policy Title:	07h E-Safety Policy
Version Number:	20210210
Approved By:	The Board
Date Approved:	26 May 2021
Date to be reviewed:	26 May 2022
Point of Contact (Reviewer):	

1.0 INTRODUCTION

Schedule for Development/Monitoring/Review

- Reviewed annually or in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place.
- Serious e-safety incidents are notified to the designated safeguarding lead and, if appropriate, the police

2.0 OUR APPROACH TO E-SAFETY

Loughborough High School believes that as part of the school's aim to equip pupils to be active citizens of the 21st century we need to educate them about the on-line world. This education takes place through a variety of routes including PSHCE and IT lessons and occasional events. Resources from outside bodies, like CEOPS and NSPCC, are used as well as internally produced material.

Good standards of behaviour and mature, responsible, considerate attitudes are expected of pupils in school and it is important that these same values are applied to their use of technology. We believe that the benefits offered by use of the internet far outweigh the problems caused by abuse and that virtually every aspect of digital technology can have educational value. The rapidly changing landscape of the digital world makes it important for pupils to be informed and responsible about keeping themselves up to date about new innovations and the opportunities and risks they present. They should also adopt a mature attitude in terms of informing the school about new and potentially harmful developments. The school community can then respond in a timely and appropriate manner.

Pupils are taught to appreciate that the internet is a public place and that everything they do on-line leaves a footprint which may be seen by those they meet, now and in later life. They are encouraged to create a positive digital profile, exercise care in selecting the material they upload and the messages they send, even in areas where privacy options can be used and security is in place. Pupils are made aware of the deceptions which can be practiced in the virtual world and encouraged to be cautious in their treatment of people and organisations they deal with electronically.

It is important that the virtually instant nature of on-line communication is not allowed to generate misunderstanding and conflict which could be avoided by a delay for thought before responding. Pupils need to be reflective and consider their actions carefully before responding. The school pastoral system deals with on-line problems as well as other e-safety concerns.

Although the school internet system is protected by filtering, pupils are made aware that this is never totally effective and that undesirable material, including malware and offensive images can get through. They are expected to report issues of this type to a member of staff as soon as possible.

Pupils are made aware of the legal restrictions surrounding on-line behaviour. They are informed of the sources of support, both within school and from outside bodies, available to deal with any problems which may occur, including cyber-bullying, on-line grooming and radicalisation. Misbehaviour is dealt with in line with the school discipline and behaviour policies.

3.0 DEVELOPMENT/MONITORING/REVIEW OF THIS POLICY

This e-safety policy has been developed by:

- ICT staff: Mrs Winship
- Assistant Head Curriculum: Mrs Connick

In this policy's development the following groups were consulted:

- LHS Senior Leadership Team
- ICT Reps

4.0 SCOPE OF THE POLICY

This policy applies to all members of the school community who have access to and are users of school ICT systems, both in and out of the school. The Education and Inspections Act 2006 empowers the Head to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school.

5.0 ROLES AND RESPONSIBILITIIES

Governors

Governors are responsible for the approval of the e-safety policy and for reviewing the effectiveness of the policy. This will be carried out by the governor responsible for e-safety.

Head and Senior Leadership Team

The Head is responsible for ensuring the safety (including e-safety) of members of the school community, though the day-to-day responsibility for e-safety will be delegated to the Head of LSF Computer Science.

Head of LSF Computer Science

- Co-ordinate the e-safety curriculum across the schools
- Liaising with safeguarding leads and coordinating the e-safety aspects of the curriculum to ensure they reflect the needs of the students.
- Advising senior staff on effective policies and training for staff and pupils regarding e-safety and cyber-bullying.

Network Manager and Network Services

The network manager and network services are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required e-safety technical requirements
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy is applied and updated on a regular basis
- that the use of the network/remote access/email/internet access is logged so that the e-safety coordinator can investigate any individual for pastoral action
- that monitoring systems are implemented and updated as agreed in school policies

Teaching and Support Staff

Teaching and support staff are responsible for ensuring that:

- they have an up-to-date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the staff responsible use policy (RUP)
- they report any suspected misuse or problem to the e-safety coordinator for investigation
- all digital communications with pupils/parents/carers should be on a professional level and only carried out using official school systems
- e-safety issues are embedded into relevant aspects of the curriculum and other activities
- pupils understand and follow the e-safety and responsible use policies
- pupils have a good, age appropriate, understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they actively monitor the use of digital technologies, mobile devices, cameras and other mobile devices in lessons and during other organised school activities and implement school behaviour and discipline policies where necessary
- staff and pupils should report unsuitable material found during internet searches to network services so that the filtering system can be fine-tuned
- Student devices in Years 7, 8, 9, 10 and 11 are managed, so regular checks can be made to the loaned devices.

Designated Safeguarding Lead
This person is trained in e-safety issues and is aware of the potential for safeguarding issues that may arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential incidents of grooming
- cyber-bullying

Pupils

- pupils are responsible for using the school systems in accordance with the responsible use and e-safety policy.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials to a member of staff as soon as possible
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's e-safety policy covers their actions out of school whilst on a school loaned device

Parents/Carers
Parents/Carers play a crucial role in ensuring that their children understand the need to use digital technologies in an appropriate way. The school will take every opportunity to help parents understand these issues, some examples of how this may be done are: online training, parents' evenings, newsletters, letters and the school website and encourage them to support the school in promoting good e-safety practice.

6.0 POLICY STATEMENTS

Education – pupils
E-safety is relevant to all areas of the curriculum and school staff reinforce e-safety messages in all subjects. Education is provided in the following ways:

- A planned e-safety curriculum is provided as part of ICT and PSHCE and is regularly revisited
- Pupils are taught to be critically aware of the content they access on-line and guided to validate the accuracy of information.
- Staff act as good role models in their use of digital technologies, the internet and mobile devices
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the network services can temporarily remove these sites from the filtered list for the period of study.

Education – parents/carers
Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of their children's on-line behaviour. The school will seek to provide information and awareness to parents and carers through: online training, parents' evenings, newsletters, letters and the school website and encourage them to support the school in promoting good e-safety practice.

Education and Training – Staff/Volunteers
Training will be offered to staff so they understand their responsibilities.

- All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and the responsible use policy.
- This e-safety policy and its updates will be presented to and discussed in staff meetings as appropriate.
- Advice/guidance/training to individuals will be supplied as required.

Technical – infrastructure/equipment, filtering and monitoring
The LSF director of network services is responsible for ensuring that the school network is as safe and secure as is reasonably possible and that policies are in place for all technical areas.

Bring Your Own Device (BYOD)

Staff and pupils are allowed to use personal devices on the LSF wifi system. This is subject to the appropriate responsible use policy.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. This is covered by the responsible use and e-safety policies.

Social Media

Social media provides educational opportunities as well as the risk of personal information becoming publicly available. Staff and pupils are encouraged to create a positive digital profile in accordance with the staff code of conduct and the appropriate responsible use policy. Issues associated with this are discussed at staff meetings and through PSHCE.

Appendix 1

Legal Framework – some guidelines and useful information

Racial and Religious Hatred Act 2006
This act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Criminal Justice Act 2003
Section 146 of the Criminal Justice Act 2003 came into effect in April 2005, empowering courts to impose tougher sentences for offences motivated or aggravated by the victim's sexual orientation in England and Wales.

Sexual Offences Act 2003
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). This can include images taken by and distributed by the child themselves (often referred to as "sexting"). A person convicted of such an offence may face up to 10 years in prison. The offence of grooming is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Anyone who has sexual intercourse with a child under the age of 13 commits the offence of rape.

Communications Act 2003 (section 127)
Sending by means of the internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Data Protection Act 2018
The act requires anyone who handles personal information to ensure that the Data Protection Principles are observed.

The Computer Misuse Act 1990 (sections 1 - 3)
Regardless of an individual's motivation, the act makes it a criminal offence to:

- Gain access to computer files or software without permission (for example using someone else's password to access files)
- Gain unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- Impair the operation of a computer or program (for example caused by viruses or denial of service attacks).
- UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)
This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988
Copyright is the right to prevent others from copying or using his or her "work" without permission. The material to which copyright may attach (known in the business as "work") must be the author's own creation

and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 — 29)
This act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Obscene Publications Act 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Regulation of Investigatory Powers Act 2000
The Regulation of Investigatory Powers Act 2000 (RIP) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998.
The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

Education and Inspections Act 2006
Education and Inspections Act 2006 outlines legal powers for schools which relate to cyberbullying/bullying:

- Headteachers have the power "to such an extent as is reasonable" to regulate the conduct of pupils off site.
- School staff are able to confiscate items such as mobile phones etc… when they are being used to cause a disturbance in class or otherwise contravene the school Anti-bullying policy.

E-safety contacts and references
CEOP (Child Exploitation and Online Protection Centre): **www.ceop.police.uk**
Childline: **www.childline.org.uk**
Childnet: **www.childnet.com**
Digizen: **www.digizen.org.uk**
Internet Watch Foundation (IWF): **www.iwf.org.uk**
Kidsmart: **www.kidsmart.org.uk**
Think U Know website: **www.thinkuknow.co.uk**
Virtual Global Taskforce — Report Abuse: **www.virtualglobaltaskforce.com**

Appendix 2

During periods of time where Loughborough High School is delivering learning through the Virtual School we are aware that both pupils and staff are on devices for longer periods of time.

Pupils have been advised of appropriate behaviour whilst online during the Virtual School and in the subsequent chats.

Staff have been trained in the use of technologies in the Virtual School and respond appropriately and quickly to new and emerging technologies.