

E-Safety Policy

Publication Date	16/05/2025
Version Number	1.0
Policy Owner	Deputy Principal Student Experience & Inclusion
Approval Level (committee)	Policy Procedure and Document Committee
Approval	Trust Board
Applies To (job roles relevant to)	This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school
Next Review Due	30.4.2027
Equality Impact Assessment	

Policy Purpose: *This policy is based on the Department for Education’s (DfE) statutory safeguarding guidance, Keeping Children Safe in Education. It also refers to the DfE’s guidance on protecting children from radicalisation. Appendix A contains a complete list of the relevant legislation.*

Main body of policy:

1. Introduction

Lighthouse Learning Trust recognises the benefits and opportunities which new technologies offer to teaching and learning. We provide internet access to all learners and staff and encourage the use of technologies in order to enhance skills, promote achievement and enable lifelong learning. However, the accessibility and global nature of the internet and the different technologies available mean that we are also aware of potential risks and challenges associated with such use. Our approach is to implement appropriate safeguards within the college while supporting staff and learners to identify and manage risks independently and with confidence.

We believe this can be achieved through a combination of security measures, training, guidance and implementation of our policies. In furtherance of our duty to safeguard learners we will do all that we can to make our learners and staff stay e-safe and to satisfy our wider duty of care.

The Trust recognises the importance of educating and protecting students from online risks, and our e-safety policy is structured around the "four Cs" framework: **Content, Contact, Conduct, and Commerce**. We are committed to ensuring that learners are safeguarded from exposure to harmful or inappropriate content; from unsafe or exploitative contact with others online; from engaging in or being affected by unacceptable conduct such as cyberbullying; and from commercial risks including scams, phishing, and age-inappropriate advertising. Through a combination of curriculum delivery, staff training, and robust filtering and monitoring systems, the Trust aims to foster a safe and responsible digital environment for all students and staff.

This e-safety policy encompasses safeguarding, acceptable use, e-Security, anti-bullying, disciplinary, digital literacy and child protection. It should be read alongside other relevant college policies.

2. Creation, Monitoring and Review

The impact of the policy will be monitored regularly, with a full review being carried out at least once a year by the Executive Principal, e-Safety Officer and Designated Safeguarding Leads.

The policy will also be reconsidered where particular concerns are raised or where an e-safety incident has been recorded.

3. Policy Scope

The e-Safety Policy applies to all use of the internet and forms of electronic communication such as email, mobile phones, social media sites and any other digital service where you are identifiable as a member of the College community.

The policy applies to all users/all learners and staff/all members of the college community. Any user of college IT systems, both on the premises and remotely, must adhere to and sign a hard copy of the IT Acceptable Use Policy.

4. Behaviour

Lighthouse Learning Trust will ensure that all users of technologies adhere to the standard of behaviour as set out in the IT Acceptable Use Policy, Code of Practice/Student Support and Disciplinary Policy.

The college will not tolerate any abuse of IT systems. Whether offline or online, communications by staff and learners should be courteous and respectful at all times.

Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and in line with the Student Support Policy and Code of Practice.

Where conduct is found to be unacceptable, the college will deal with the matter internally.

Where conduct is considered illegal (see Appendix A for relevant legislation), the college will report the matter to the police.

Accessing of sites linked to extremist or radical views/behaviour will be dealt with in accordance with the College's Safeguarding Policy.

5. Roles and Responsibilities

All members of the college community should know their responsibilities for e-safety.

Below are the roles and responsibilities relevant within this college:

E-Safety Officer:

The e-Safety Officer is responsible for keeping up to date with new technologies and their use, as well as attending relevant training. The e-Safety Officer is IT Director.

The e-Safety Officer is responsible for updating the e-Safety Policy to keep up with technological advancements.

Designated Safeguarding Lead (DSL):

DSL is expected to deliver staff development and training and liaise with the local authority and external agencies to promote e-safety within the college community.

All e-safety incidents will be recorded by the Designated Safeguarding Lead using an agreed format.

Learners:

Learners are responsible for using any IT systems and mobile devices in accordance with the college IT Acceptable Use Policy for Students, which they must sign.

Learners must always act safely and responsibly when using the internet and/or mobile technologies, and online platforms.

All learners must complete an e-safety tutorial during induction. This will include the understanding that social media is an important tool in the sharing of extreme material and that extremist groups are actively using social media to inform, share propaganda, radicalise and recruit for their cause. It will also include information on what students should do if they have e-safety concerns (including to whom they must report any terrorist-related online material). In most cases, this will be their tutor.

Students are responsible for attending further e-safety training as part of the curriculum and are expected to know and act in line with other relevant college policies while using mobile phones, sharing images etc.

Staff:

All staff are responsible for using any IT systems and mobile devices in accordance with the college's Acceptable Use of IT Policy for staff, which they must sign.

Staff are responsible for attending staff training on e-safety and displaying a model example to learners at all times through embedded good practice.

Any digital communication between staff and learners or parents/carers (e.g. email, messaging via online platforms, text message via ProSolution) must be professional in tone and content in line with the college's Acceptable Use of IT Policy. These communications may only take place on official (monitored) college systems.

Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.

All staff should apply relevant college policies and understand the incident reporting procedures. Any e-safety-related incident that is reported to or discovered by a staff member must be reported to the line manager and Designated Safeguarding Lead, e-safety Officer without delay – before the end of the working day, who may then report to the Vice Principal.

When informed about an e-safety incident, staff members must take particular care not to guarantee any measure of confidentiality towards either the individual reporting it, or to those involved.

Where management considers it appropriate, the child protection officer may be asked to intervene with appropriate additional support from external agencies.

External customers:

Where college facilities have been let to external agencies, information regarding e-safety will be communicated, and this policy will apply.

6. Security

The college is taking steps to ensure the safety and security of its network. This includes implementing enhanced web filtering, keystroke monitoring, and other forms of protection to prevent accidental or malicious access to college systems and information.

Digital communications over the college network, such as email and internet postings, web searching and usage, will be monitored in accordance with the IT Acceptable Use Policy.

7. Risk Assessment

In making use of new technologies and external online platforms, all staff must liaise with the e-safety Officer, who will carry out an e-safety risk assessment.

Staff should complete a Data Protection Impact Assessment (DPIA) if the new online platform poses a risk to individuals' personal data.

8. Communications

Lighthouse Learning Trust requires all users of IT to adhere to College guidelines when using email, mobile phones, social media sites, game consoles, chatrooms, video conferencing and using web cameras.

Use of social media at College

Students are permitted to make reasonable and appropriate use of social media websites where this is part of the normal work relating to their studies. The College accepts that students may wish to use social media channels as a way of communicating personally with other students, the public and/or friends; however, its use at the College should be restricted to the terms of this policy.

Students who are responsible for contributing to the College's social media activities should be aware at all times that they are representing the College.

Selected student groups are permitted to make reasonable and appropriate use of social media websites from the College's IT network at certain times or from selected college workstations at the discretion of Curriculum Managers.

Access to certain social media sites may be blocked during normal College working hours at the discretion of the senior management team.

Students may wish to use their own personal devices, (including laptops, hand-held devices and smartphones) to access social media websites, while at College. Students should limit their use of social media to break/lunch times and/or when travelling (before and after College) unless directed to access such a site for educational purposes.

Personal use of social media should not interfere with students' studies and responsibilities.

Abuse of this policy will be considered a disciplinary offence as outlined in the Student Behaviour Policy.

9. Use of Images and Video

All learners and staff should receive training on the risks when taking, downloading and posting images online and making them available to others. There are particular risks where personal images of themselves or others are posted onto social networking sites.

College teaching staff will provide information to learners on the appropriate use of images and videos. This includes photographs of learners and staff as well as using third-party images.

Photographs of activities on the college premises should be considered carefully and have the consent of individuals being photographed before being published. Approved photographs should not include names of individuals without consent.

Learners are not permitted to record audio or video of lessons and other college-based activities in any form for their own purposes or for the purposes of others unless in exceptional circumstances where they have asked for and been given permission to do so by the teacher.

Where permission has been given to video, any images should not be forwarded, published, amended or placed on any electronic media platform without the explicit authorisation of the person/people on the images.

Using images or videos in teaching and learning is a common practice and should be promoted, as long as it does not violate any copyright or other rights of a third party, such as image rights or personal data rights. This includes images obtained from the internet as well as those owned by staff or students.

10. Online Commerce and Financial Security

Lighthouse Learning Trust acknowledges that the internet is a platform for commercial activities, including online shopping, banking, and in-app purchases. While these can offer convenience, they also present risks such as financial fraud, identity theft, and exposure to scams. The college aims to educate its community on safe online commercial practices.

Learners and staff should be aware of the potential financial risks when engaging in online transactions or interacting with commercial content. This includes understanding the dangers of phishing scams (fraudulent attempts to obtain sensitive information like usernames, passwords, and credit card details), malware designed to steal financial data, and misleading advertising.

When any online financial transactions are necessary for educational purposes through college-approved platforms, the college will ensure that secure payment methods are used. For personal transactions, learners and staff are advised to:

- Only use reputable and secure websites for purchases (look for "https" and a padlock symbol in the browser address bar).
- Avoid using public Wi-Fi for financial transactions.
- Regularly monitor bank and card statements for any unauthorised activity.

Learners and staff must be vigilant about protecting their personal financial information online. This includes:

- Never sharing bank account details, credit card numbers, or online banking passwords via email, social media, or unverified websites.
- Being cautious of unsolicited emails or messages asking for financial information or prompting urgent action.
- Using strong, unique passwords for online accounts, especially those linked to financial information.

Learners should be particularly mindful of in-app purchases and financial elements within online games. Parental/carer consent and oversight are crucial for any expenditure by underage learners. The college network may restrict access to games or platforms with significant financial risk or gambling-like mechanics.

Any suspected online financial scams or fraud encountered using college IT systems, or that impact a member of the college community in a way that relates to their college life, should be reported to the e-Safety Officer or Designated

Safeguarding Lead. The college will provide support and direct individuals to appropriate external agencies, such as Action Fraud, where necessary.

Learners and staff should be critical of online advertising and endorsements. It is important to understand that not all advertised products or services are legitimate or safe. The college does not endorse any third-party products or services advertised on external websites accessed via its network unless explicitly stated.

11. Personal Information

Any processing of personal information needs to be done in compliance with the Data Protection Act 1998/ General Data Protection Regulation ((EU) 2016/679) (GDPR) and we will process and store in accordance with the legislation. This includes content such as learner records, e-portfolios and assessed work.

No personal information can be posted to the college website unless it is in line with our Data Protection Policy. Only names and work email addresses of senior staff will appear on the college website. No other staff/ learners' personal information will be available on the website without consent.

Staff must keep learners' personal information safe and secure at all times e.g. when using online platforms.

12. Education and Training

The college will support staff and learners to stay safe through regular training and education. This will provide individuals with skills to be able to identify risks independently and manage them effectively.

Learners will receive training in online e-safety during induction. Follow-up training will be carried out as appropriate as part of the tutorial system. Issues associated with e-safety apply across the curriculum and learners should receive guidance on what precautions and safeguards are appropriate when making use of the internet and technologies. Within classes, learners will be encouraged to question the validity and reliability of materials researched, viewed or downloaded. They will also be encouraged to respect the copyright of other parties and to cite references properly.

Learners will be informed who to talk to when they have concerns about inappropriate content, either where that material is directed to them, or where it is discovered as part of a random search.

The college e-Safety Rules (Appendix B) will appear when users log on to the college network and these rules are highlighted in posters and leaflets around IT areas and workstations.

Staff will take part in mandatory e-safety training before beginning a new college year lead by DSL.

Any new staff will receive training on the college IT system, led by the e-safety Officer, during staff induction.

13. E-safety Incidents and Response

When an e-safety incident is reported to the college, the college will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring.

Learners can report an incident, to their personal tutor, college e-Safety Officer or Designated Safeguarding Lead.

Staff members can report an incident to their line manager or Designated Safeguarding Lead or e-safety Officer as soon as possible (before the end of the working day). In all cases Designated Safeguarding Lead must be informed by the incident being recorded on CPOMs.

Following any incident, the college will review what has happened and decide on the most appropriate and proportionate course of action. Sanctions may be put in place, external agencies may be involved or the matter may be resolved internally depending on the seriousness of the incident.

Serious incidents will be dealt with by senior management, in consultation with appropriate external agencies.

14. Feedback and Further Information

Lighthouse Learning Trust welcomes all constructive feedback on this and any other college policy. If you would like further information on e-safety or wish to send us your comments on our e-safety Policy, then please contact the Principal.

APPENDIX A

Legislation

Schools should be aware of the legislative framework under which this E-Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online. It is recommended that legal advice is sought in the advent of an e safety issue or situation.

DfES 'Keeping Children Safe in Education'

Statutory guidance for schools and colleges

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998, General Data Protection Regulation ((EU) 2016/679) (GDPR)

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Counter-Terrorism and Security Act 2015

The Prevent strategy addresses all forms of terrorism and we continue to prioritise according to the threat they pose to our national security; the allocation of resources

will be proportionate to the threats we face. The Prevent strategy has three specific strategic objectives:

1. Respond to the ideological challenge of terrorism and the threat we face from those who promote it;
2. Prevent people from being drawn into terrorism and ensure that they are given appropriate advice and support;
3. Work with sectors and institutions where there are risks of radicalisation that we need to address.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

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.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;

- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

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.

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.

Protection of Children Act 1978

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). A person convicted of such an offence may face up to 10 years in prison.

Sexual Offences Act 2003

The new grooming offence 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. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

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. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of Pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

APPENDIX B

E-Safety Rules

1. Always think of your personal safety first when using ICT or your mobile phone. Remember it is easy for anyone to lie about who they are online, so you can never really be sure about who you are talking to.
2. Do not give out any personal information about yourself online to people you do not know. This includes your full name, address, street name, postcode, or school name.
3. Only ever give out your general location (e.g. as Southampton, Gosport).
4. Never give your contact number to anyone who you don't know.
5. Use a nickname rather than your real name.
6. Don't meet people that you have only spoken to online. If you do decide to meet up with anyone in real life then make sure you take a trusted adult with you and meet in a public place at a busy time.
7. Never give out pictures online or over a mobile unless you know the person in real life. It is easy for people to take your pictures and alter them, send them on, or even pretend to be you with them.
8. Always use private settings whenever you are setting up a social networking page or an Instant Messenger (IM) account. This is so people who you don't want to see your profile can't. Anything you post or upload to the internet is there forever so be very careful what you put online.
9. Never go onto webcam with people you don't know in real life. Webcam images can be recorded and copied and also shared with other people.
10. If you receive any messages or pictures that worry or upset you talk to an adult you trust. You may also report it online, via the thinkuknow website <http://www.thinkuknow.co.uk>

Links to other policies:

BYOD Policy for Students, Data Protection Policy, Student Behaviour Policy and Student Code of Conduct

Document History

Version	Approved by	Date Approved
V1	PPD	13.5.2025