Online Safety Policy

Policy Owner:	Lighthouse Multi Academy Trust
Approved/ Ratified:	Pat Hunt
Review Dates:	February 2027

Version Control Log

Version	Modification Date	Synopsis of Changes
1.0	September 2025	
2.0	December 2025	AUP reviewed for Staff and Volunteers following GDPR audit and amended accordingly (Appendix 3) AUP developed for Governors/ Trustees and Members (Appendix 7) Taken to Trustees Feb 2026

Key Contacts for Online Safety	
Designated Safeguarding Lead (DSL), with lead responsibility for filtering and monitoring	Sarah Corkindale scorkindale@lhmat.com
Deputy Designated Safeguarding Leads / DSL Team Members	Nanette Broadway nbroadway@sunshine.lhmat.com Rebecca Taylor rtaylor@sunshine.lhmat.com
Lighthouse Multi Academy Trust Director for Safeguarding and Attendance	Richard Rose rrose@lhmat.com
Link governor for safeguarding and Attendance	Safeguarding & Online Safety: Vicki Taylor vtaylor@sunshine.lhmat.com Attendance & Online Safety: Jane Freeth jfreeth@sunshine.lhmat.com
Curriculum leads with relevance to online safeguarding and their role [e.g. PSHE/RSHE/RSE/Computing leads]	Computing and Online Safety Lead: Melanie Hindley mhindley@sunshine.lhmat.com PSHE/RSE Lead: Rebecca Taylor rtaylor@sunshine.lhmat.com
Network manager / other technical support	LA ICT enquiries@la-ict.com

Introduction

This includes reference to the fact that academies may wish to restrict access to mobile devices in academy, in acknowledgement of the fact that children have "unlimited and unrestricted access to the internet" which may facilitate abuse in the academy.

The Lighthouse Multi Academy Trust recognises the role of IT and the internet as part of the statutory curriculum and a necessary tool for learning. This policy also reflects the requirements of Keeping Children Safe in Education (KCSiE) 2025 Sections 134 – 151 of Part 2 (pages 38 - 41) which sets out substantial guidance including remote learning, filters and monitoring, information security, cyber-crime, reviewing online safety provision and information and support.

The safe and appropriate use of technology results from a co-ordinated approach between curriculum leadership, safeguarding leadership, and network management. This policy reflects key responsibilities in ensuring this and should be read in conjunction with other Trust policies including:

- Data Protection Policy
- Acceptable Use Policies for Staff and Pupils
- Mobile Phone Policy incorporated into the Lighthouse Multi Academy Trust Code of Conduct
- Local Academy CCTV Policy
- The Lighthouse Multi Academy Trust Staff Code of Conduct
- The Lighthouse Multi Academy Trust Safeguarding and Child Protection Policy
- The Lighthouse Multi Academy Trust Child on Child, Sexual Harassment and Sexual Violence Policy

The Trust undertakes to:

- Ensure that policies on mobile and smart technology are reflected in its child protection policy (KCSiE para 137). This includes giving due and reasonable consideration to the potential necessity identified in KCSiE to

restrict access to mobile devices in the academy in acknowledgement of the fact that children have "unlimited and unrestricted access to the internet" which may facilitate abuse in the academy.
- Annually review and develop this e-safety policy in line with new legislation, technologies and incidents.
- Ensure regular, documented audit of academies technical infrastructure Provide academies with online monitoring mechanisms so that incidences of misuse and abuse can be detected, investigated and responded to appropriately in a timely manner.
- Ensure all academies complete an annual online safety audit.

Introduction

The Online Safety Policy is part of our suite of safeguarding policies and relates to other policies including those for behaviour, social and health education (PSHE) Any issues and concerns with online safety must follow the academy safeguarding and child protection procedures.

It is the duty of our academies to ensure that every child in our care is safe and the same principles should apply to the 'virtual' or 'digital' world as would normally be applied to our day to day safeguarding procedures.

Scope of the Policy

This policy applies to all members of The Lighthouse Multi Academy Trust community (including staff, pupils, volunteers, parents /carers, visitors and community members) who have access to and use the digital technology systems, both in and out of the academies.

Our academies will deal with such incidents within this policy and associated behaviours and anti-bullying policies and will, where known, inform parents/ carers of incidents of inappropriate Online Safety behaviour that takes place outside of the academies.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

Content: being exposed to illegal, inappropriate or harmful material; for example

pornography, fake news, racist or radical and extremist views, hate content and content

validation, how to check authenticity and accuracy of online content; and

Contact: being subjected to harmful online interaction with other users; for example commercial advertising, grooming (sexual exploitation, radicalisation etc.), online bullying in all forms and social or commercial identity theft, including passwords; and

Conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, online bullying, health and wellbeing, consensual and non-consensual sharing of nude and semi-nude image and copyright.

Commerce: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk. The Lighthouse Multi Academy Trust has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

Aim

The Lighthouse Multi Academy Trust has robust processes in place to ensure the online safety of pupils, staff, volunteers, Governors and Trustees.

We aim to:

Deliver an effective approach to online safety, which empowers us to protect and

educate the whole community in its use of technology.

- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate
- Provide early identification and early intervention
- Set out clear expectations for all Lighthouse Multi Academy Trust community members' online behaviour, attitudes and activities and use of digital technology.
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the academy gates and academy day, and regardless of device or platform
- Facilitate the safe, responsible and respectful use of technology to support teaching and learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- Help our staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns (with reference to other Lighthouse Multi Academy Trust policies and procedures.

Legislation and Guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for academies on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation, Teaching Online Safety in Schools, Harmful Online Challenges and Online Hoaxes, the sharing of misinformation and guidance on sharing of nudes and semi nudes.

This Online Safety Policy must be read in conjunction with the following Lighthouse Multi Academy Trust Policies:

- Acceptable Use Policy
- Academy Behaviour Policy
- Academy Safeguarding and Child Protection Policy
- The Lighthouse Multi Academy Trust Code of Conduct
- The Lighthouse Multi Academy Trust Child on Child, Sexual Violence and Sexual Harassment Policy

Roles and Responsibilities

The following section of the policy outlines the Online Safety roles and responsibilities of individuals and groups across The Lighthouse Multi Academy Trust.

Governors and Trustees at the Lighthouse Multi Academy Trust

As we continue to use online platforms to work and collaborate, it is essential that children are safeguarded from potentially harmful and inappropriate online material. As such, Trustees and Governors should ensure appropriate filters and appropriate monitoring systems are in place.

The Board of Directors has overall responsibility for monitoring this policy and holding the CEO/ and Executive Headteachers/Headteachers to account for its implementation.

The Local Governing Bodies are responsible for monitoring and the implementing of the policy at a local Academy level, they will coordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the Designated Safeguarding Leads (DSL).

All Trustees and Governors will:

- Ensure that they have read and understood the policy
- Agree and adhere to the terms set out under the Lighthouse Multi Academy Trust ICT Acceptable Use and Information Security policies
- Reporting to relevant Governors meetings
- Attend Governor and Director Training which includes Online Safety
- Ensure that they have a good understanding of the filtering and monitoring processes and its effectiveness within the academy and across The Lighthouse Multi Academy Trust
- The Safeguarding and Attendance Link Governor will be the nominated member of the governing body to have responsibility for filtering and monitoring at their designated academy

Executive Headteachers/Headteachers and/or Head of School

The Executive Headteacher/Headteacher or Head of School are responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout their own Academy within The Lighthouse Multi Academy Trust.

- The Executive Headteacher/Headteacher or Head of School has a duty of care for ensuring the safety (including online safety) of members of the academy community, though the day to day responsibility for online safety may be delegated to the Online Safety Lead in each academy.
- Foster a culture of vigilance and fully integrated across the Academy
- Oversee the activities of the Designated Safeguarding Lead and ensure that the DSL responsibilities listed below in the section are being followed and fully supported
- Ensure that policies and procedures are followed by all staff
- Undertake training in offline and online safeguarding, in accordance with statutory guidance and relevant Safeguarding Partners guidance
- Audit the quality of online safety across the academy on an annual basis
- Liaise with the Designated Safeguarding Lead on all online safety issues, which might arise and receive regular updates on wider MAC issues and broader policy and practice guidance.
- Take overall responsibility for data management and information security ensuring that The Lighthouse Multi Academy Trust provision follows best practice in information handling, work with the DPO, DSL, Directors and Governors to ensure a GDPR compliant framework for storing data, but helping to ensure that child protection is always put first and data-protection processes support careful and legal sharing of information
- Be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and online safety roles
- Understand and make all staff aware of procedures to be followed in the event of a serious online safeguarding incident
- Ensure suitable risk assessments are undertaken so the curriculum meets the needs of pupils, including risk of children being radicalised
- Ensure that there is a system in place to monitor and support staff who carry out internal online-safety procedures
- Ensure Directors and Governors are regularly updated on the nature and effectiveness of The Lighthouse Multi Academy Trust arrangements for online safety and report the number of online safety notifications through the Headteacher's Report to governors
- Ensure that Academy websites meet statutory DfE requirements

The Online Safety Lead and the Designated Safeguarding Lead

The Online Safety Lead, alongside the DSL takes lead responsibility for online safety in each academy, in particular:

- Supporting the Executive Headteacher/Headteacher or Head of School in ensuring that staff understand the policy and that it is being implemented consistently throughout the academy
- Working with the CEO, Lighthouse Leadership, Academy Leaders, IT staff and other staff as necessary, to address any online safety issues or incidents
- Ensuring that any online incidents (including those through monitoring notifications) are logged on CPOMS and dealt with appropriately in line with this policy. These CPOMS Incidents must be logged under 'Online Safety' outlining the action taken by the Designated Safeguarding Lead
- Ensuring that incidents of cyber-bullying are logged and dealt with appropriately in line with the academy's Behaviour and Anti-Bullying Policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in the Academy to the Director of Safeguarding and Attendance and Lighthouse Multi Academy Trust Trustees
- **The Designated Safeguarding Lead should take responsibility for safeguarding and child protection (including online safety)**
- **Where the online safety lead is not the named DSL or Deputy DSL, ensure there is regular review and open communication between these roles and that the DSL's clear overarching responsibility for online safety is not compromised**
- Ensure an effective approach to online safety that empowers our academies to protect and educate the whole community in their use of technology and establishes mechanisms to identify, intervene and escalate any incident where appropriate.
- Liaise with the Local Authority and work with other multi agency professionals in line with Working Together to Safeguard Children
- Take day to day responsibility for online safety issues and be aware of the potential for serious child protection concerns
- Stay up to date with the latest trends in online safety
- Receive regular updates in online safety issues and legislation, be aware of local and academy trends
- Ensure that online safety education is embedded across the curriculum and beyond
- Promote an awareness and commitment to online safety through The Lighthouse Multi Academy Trust, with a strong focus on parents, who are often appreciative of academy support in this area, but also including hard-to-reach parents
- Liaise with IT, pastoral and support staff as appropriate
- Communicate regularly with other SLT members and Safeguarding Link Governor to
- Discuss current issues (anonymised as appropriate), review incident logs and discuss filtering and monitoring
- Ensure all staff are aware of the procedures that need to be followed in the event of an online safety incident, and that these are logged in the same way as any other safeguarding incident
- Ensure DfE guidance from Keeping Children Safe in Education is followed.
- The Designated Safeguarding Lead should take responsibility for the filtering and monitoring processes within the academy. Monitoring alerts will be sent to the DSL and DDSL for the individual academy and should be recorded in accordance with policy.
- Facilitate training and advice for all staff

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of the policy
- All staff and volunteers will receive an update in regards to filtering and monitoring on induction.
- All staff and volunteers will have an understanding of the filtering and monitoring processes at the academy
- Implementing this policy consistently
- Agreeing and adhering to the Lighthouse Multi Academy Trust ICT Acceptable Use Policy
- Working with their local academies to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensure that any incidents of cyber-bullying are dealt with appropriately in line with local Academy behaviour policy
- Understand that online safety is a core part of safeguarding; as such it is part of everyone's job- never think that someone else will pick it up
- Know who the Designated Safeguarding Leads (DSL) and Online Safety Lead (OSL) ar
- Read Part 1 of Keeping Children Safe in Education
- Read and follow this policy in conjunction with the Academy safeguarding and child protection policy
- Record online safety incidents in the same way as any safeguarding incident and report through CPOMS
- Understand that safeguarding is often referred to as a jigsaw puzzle – you may have discovered the missing piece so do not keep anything to yourself
- Notify the DSL or Online Safety lead if the policy does not reflect practice in your local academy and follow escalation procedures if concerns are not promptly acted upon
- Identify opportunities to thread online safety through all activities, both outside the classroom and within the classroom
- To carefully supervise and guide pupils when engaged in learning activities involving online technology, supporting them with search skills, critical thinking (e.g fake news or the sharing of misinformation), age appropriate materials and signposting
- Notify the DSL or Online Safety Lead of new trends and issues before they become a problem
- Take a zero tolerance approach to bullying and sexual harassment
- Be aware that you are often most likely to overhear online-safety issues (particularly relating to bullying and sexual harassment and violence) in the playground, corridors, toilets and other communal areas outside the classroom- let the DSL/ Online Safety Lead know
- Receive regular updates from the DSL and Online Safety Lead and have professional curiosity for online safety issues
- Model safe, responsible and professional behaviours in their own use of technology in line with The Lighthouse Multi Academy Trust Acceptable Use Policy.

Pupils

Throughout the course of a pupil's time within The Lighthouse Multi Academy Trust, pupils will be taught about online safety throughout the curriculum:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact, conduct and commerce and identify a safe adult to report their concerns
- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns and identify a 'safe adult' to speak to in each Academy

- Understand the importance of adopting good online safety practice when using digital technologies/mobile devices outside of the academy community (including the use of 3G/4G and 5G devices) and realise that online safety covers their actions out of academy.

Parents

The Lighthouse Multi Academy Trust recognises that parents play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way.

The Lighthouse Multi Academy Trust will take every opportunity to help parents understand these issues through parents' meetings, newsletters, letters, website, social media and information about national/local online safety campaigns/ literature. Parents and carers will be encouraged to support The Lighthouse Multi Academy Trust in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Notify members of academy staff if they have any concerns or queries in regards to their child's online safety at the earliest opportunity.

Data Protection Officer

The Lighthouse Multi Academy Trust will ensure that arrangements will reflect our responsibilities under this online safety policy.

- Be aware of references to the relationship between data protection and safeguarding in key Department for Education documents 'Keeping Children Safe in Education and 'Data Protection: a toolkit for academies (April 2018) - especially this quote from the latter document:

"GDPR does not prevent, or limit, the sharing of information for the purpose of Keeping Children Safe. Legal and secure information sharing between The Lighthouse Multi Academy Trust, Multi Agency Safeguarding Hub, and other local agencies, is essential for keeping children safe and ensuring they get the support they need.

Information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children. As with all data sharing, appropriate organisational and technical safeguards should still be in place. Remember the law does not prevent information about children being shared with specific authorities, it is for the purpose of safeguarding."

<u>Education and Curriculum</u>

The following subjects have the clearest online safety links:

- PSHE
- Relationships and Health Education
- Computing
- Citizenship

It is the role of all MAT staff to identify opportunities to thread online safety through all activities, both outside the classroom and within the curriculum, supporting curriculum/stage/ subject leads and making the most of unexpected learning opportunities as they arise.

Whenever overseeing the use of technology in any of the Academies or setting home learning, all staff should encourage sensible use, monitor what pupils are doing and consider potential dangers and the age appropriateness of websites.

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extracurricular and extended academy activities if relevant) supporting them with search skills, critical thinking (e.g fake news and misinformation) and age appropriate materials.

At The Lighthouse Multi Academy Trust, we recognise that online safety and broader digital resilience must be weaved throughout the curriculum.

Handling Online Safety Concerns and Incidents

All staff must recognise that online safety is a part of safeguarding. General concerns must be addressed in the same way as any other safeguarding concern; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should err on the side of talking to the DSL/DDSL and Online Safety Lead. Concerns must be logged using our e-safeguarding systems (CPOMS).

Academy staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets, and other communal areas outside of the classroom (particularly relating to bullying and sexual harassment and violence).

The Lighthouse Multi Academy Trust procedures for dealing with online safety will mostly be detailed in the following policies:

- Safeguarding and Child Protection Policy
- Anti Bullying Policy
- Behaviour Policy
- ICT Acceptable Use Policy
- Data Protection Policy
- Lighthouse Multi Academy Trust Code of Conduct

The Lighthouse Multi Academy Trust commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside and outside of the Academy (and that those from outside will continue to impact pupils when they come back). All staff are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively.

Any suspected online risk should be reported to the Designated Safeguarding Lead on the same day in a timely and robust manner.

Any concern/allegation about staff misuse is always referred directly to the Executive Head or Headteacher, unless the concern is about the Executive Head/Headteacher in which case the concern/allegation is referred to Chair of Governors/CEO who will liaise with the Local Authority Designated Officer (LADO). Staff may also use the NSPCC Whistleblowing Hotline.

The Lighthouse Multi Academy Trust will actively seek support from other agencies, as needed (i.e. the local authority, UK Safer Internet Centre's Professionals Online Safety Helpline, NCA CEOP, Prevent Office, IWF). We will inform parent/carers of online safety incidents involving their children, and the police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law (particular procedures are in place for the sharing of nudes and semi nudes see sections below)

Actions where there are concerns about a child

As outlined previously, online safety concerns are no different to any other safeguarding concerns. Staff with concerns about a child's safety should refer to the local academy's Safeguarding and Child Protection Policy

Consensual and non-consensual sharing of nude and semi-nude images

All Lighthouse Multi Academy Trust academies must refer to the UK Council for Child Internet Safety guidance on sexting (also referred to as ' youth-produced sexual imagery') in academies. NB – where one of the parties is over 18, this is child sexual abuse. Government guidance on sexting in academies and colleges is also available.

Online Bullying

Definition: Online Bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

To help prevent cyber-bullying, The Lighthouse Multi Academy Trust will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. Our Academies will ensure that our pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying.

All staff receive training on online bullying, its impact and ways to support pupils, as part of safeguarding training.

Our Academies also send information/ leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to specific incidents of online bullying the local Academy will follow the processes set out in the Behaviour Policy. Where illegal, inappropriate or harmful material has been spread among pupils, the Academy will use all reasonable endeavours to ensure the incident is contained.

The Executive Headteacher/ Headteacher/Head of School / Designated Safeguarding Lead will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Sexual Violence and Harassment

All staff should be aware that Keeping Children Safe in Education outlines how to keep children and young people safe from sexual violence and sexual harassment.

Any incident of sexual harassment or violence (online or offline) should be reported the DSL/DDSL who will follow the full guidance.

Staff should work to foster a zero tolerance culture. The guidance stresses that academies must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate. The document makes specific reference to behaviours such as 'upskirting' .

The Voyeurism (Offences) Act, which is commonly known as the Upskirting Act, came into force on 12 April 2019. 'Upskirting' is where someone takes a picture under a person's clothing (not necessarily a skirt) without their permission and or knowledge, with the intention of viewing their genitals or buttocks (with or without underwear) to obtain sexual gratification, or cause the victim humiliation, distress or alarm. It is a criminal offence.

Anyone of any gender, can be a victim.

All staff will follow the The Lighthouse Multi Academy Trust Managing Child on Sexual Harassment and Sexual Violence Policy and report all concerns/ niggles or worries straight away through the CPOMS system.

Harmful Online Challenges, Online Hoaxes and the Spread of Misinformation

A hoax is a deliberate lie designed to seem truthful, and online challenges generally involve users recording themselves taking a challenge, and then distributing the video through social media channels, inspiring or daring others to repeat the challenge.

The internet and social media provide a perfect platform for hoaxes, especially hoaxes about challenges or trends that are said to be harmful to children and young people to spread quickly.

Our academies will make it clear to children, young people, parents, carers and staff, in advance, what we will do when a harmful online challenge or online hoax begins to circulate. Our Academies have established mechanisms to identify, intervene and escalate incidents where appropriate.

Our academies will provide opportunities to learn to critically identify and respond to dangerous or harmful content. We are aware that some children and young people will struggle to identify harmful online challenges and online hoaxes.

Our academies will provide safe and open spaces for children and young people to ask questions and share concerns about what they experience online without being made to feel foolish or blamed. If a child, young person or adult raises a concern about a harmful online challenge or hoax directly, we will consider the best way to speak to individuals where appropriate.

We will continue to focus on what 'good online behaviour' looks like, what to do if you see something upsetting online and who and where to report it. Concerns will be followed up by the Designated Safeguarding Leads at the Academy.

Data Protection Breaches Involving Personal Devices

Where an issue is raised involving an academy or Trust data being shared, downloaded, stored, or transmitted via a personal device (including mobile phones, I-Pads/tablets, laptops/PC's, or personal email accounts), the matter will be dealt with promptly and proportionately.

The academy/Trust will:

- **Assess the nature and severity of the incident**, including the type of data involved (e.g. personal, sensitive, or special category data) and the potential risk to individuals.
- **Take immediate steps to contain the issue**, which may include requesting deletion of data, restricting access, or securing devices and accounts.
- **Investigate the circumstances** in line with the Data Protection Policy and Information Security procedures.
- **Notify the Data Protection Officer (DPO)** and, where required, consider reporting the incident to the Information Commissioner's Office (ICO) within statutory timescales.
- **Inform affected individuals** where there is a high risk to their rights and freedoms.
- **Apply appropriate actions or sanctions**, in line with staff disciplinary procedures, governor code of conduct, or contractor agreements, where policy has not been followed.
- **Provide guidance, training, or support** to prevent recurrence, recognising that incidents may arise from error as well as misuse.

All users are required to **report any suspected or actual data breach immediately**, regardless of perceived severity.

Failure to follow this policy may result in further action in accordance with the academyl/Trust procedures.

Appendix 1

EY's Online Safety
Acceptable Use Agreement

Our Technology Rules

- I will follow these rules to use computers, tablets and the internet safely at school.

Staying Safe

- My teacher will watch what I do on computers, tablets and the internet to keep me safe.
- If I see something that makes me feel worried or upset, I will tell my teacher or a trusted adult straight away.
- I will only use apps, games or websites my teacher says are safe.

Using Technology Kindly

- I will be kind when using technology, just like I am in real life.
- I will take care of the computers and tablets I use.
- I will only look at things my teacher says are OK.

Making Good Choices

- I know that I can say no / please stop to anyone online who makes me feel sad, worried or upset.
- I will ask for help from a trusted adult if I am not sure what to do or if I think I may have done something wrong.

What Happens If I Forget the Rules?

- If I forget the rules, my teacher will help me learn to make better choices next time.

These rules help us all stay safe and have fun using computers and tablets at school!

I have read and understand the above and agree to follow these rules.

Name (written by child): _____ *Date:* _____

Signed (parent/ carer): _____ *Date:* _____

Appendix 2

KS1 Online Safety
Acceptable Use Agreement

Our Technology Rules
I will follow these rules to use computers, tablets and the internet safely at school.



Staying Safe

- My teacher will watch what I do on computers, tablets and the internet to keep me safe.
- I will keep my passwords secret and tell my teacher if I need help.
- I understand that people online are not always who they say they are. I will only talk to people online if my teacher or a trusted adult says it's OK.
- I will not share my name, address, or pictures without asking my teacher or a trusted adult first.
- If I see something that makes me feel worried or upset, I will tell my teacher or a trusted adult straight away.
- I will only use apps, games or websites my teacher says are safe.

Using Technology Kindly

- I will be kind when using technology, just like I am in real life.
- I will take care of the computers and tablets I use.
- I will only look at things my teacher says are OK.

Making Good Choices

- I will ask my teacher before I use someone else's pictures or work.
- I will take breaks from screens and do other fun things too.
- I know that I can say no / please stop to anyone online who makes me feel sad, uncomfortable, embarrassed or upset.
- I will ask for help from a trusted adult if I am not sure what to do or if I think I may have done something wrong.

What Happens If I Forget the Rules?

- If I forget the rules, my teacher will help me learn to make better choices next time.

These rules help us all stay safe and have fun using computers and tablets at school!

I have read and understand the above and agree to follow these rules.

Name: _____ *Year group:* _____

Signed: _____ *Date:* _____

Appendix 3



Acceptable Use Policy (AUP): All Staff and Volunteers

Lighthouse Multi Academy Trust Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy (AUP) is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems, school data and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The Lighthouse Multi Academy Trust and academies will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for *pupils* learning and will, in return, expect staff and volunteers to agree to be responsible users.

Print and read pages 2-4, complete the declaration and pass the copy to your Executive Head Teacher/ Head Teacher / Head of School to sign and store safely. Please keep a copy of this agreement for your personal record.

LIGHTHOUSE MULTI ACADEMY TRUST	**Academy Name**		Sunshine Academy
	Staff member Name		
	AUP review Date	September	
	Review Cycle	Annually	
	Who reviewed this AUP?	Trust Central Team	
	AUP approved by	Trust Board	

Acceptable Use Agreement: All Staff and Volunteers

I understand that I must use academy systems in a responsible way, to minimise the risk to the safety, privacy or security of the academy community and its systems. I acknowledge the potential of digital technologies for enhancing learning and will endeavour to integrate them in a way that aligns with the academy's policy, ethos and values.

For my professional and personal safety:

- I understand that the academy will monitor my use of academy devices and digital technology systems.
- I understand that the rules set out in this agreement also apply to use of these devices and technologies out of the academy, and to the transfer of personal / sensitive data (digital or paper based) out of the academy. E.g academy laptops/ memory sticks/ hard drives
- I understand that the academy devices and digital technology systems are primarily intended for educational use and that I will only use them for personal or recreational use within relevant academy policies.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will store my passwords securely and in line with the academy's relevant security policy.
- If my password is compromised, I will ensure I change it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using digital technologies and systems:

- I will not access, copy, remove or otherwise alter any other user's files, without a lawful basis or their express permission and informed consent.
- I will communicate with others in a professional manner. I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the academy's policy on the use of digital/video images, and taking account of parental permissions.
- I will not use my personal equipment (e.g. personal digital cameras/I-pads, camera phones or digital devices) for taking, editing and transferring images or videos of pupils or staff, unless I have permission to do so from the Head Teacher. Where these images are published (e.g. on the academy website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in the academy in accordance with academy policies. *(These may include Academy Facebook, TikTok, Instagram, X,)*
- I am aware that if I choose to follow any of the academy/ Trust social networking sites using my personal account, my profile photo and name is visible to parents/carers who are also following.
- I will ensure my account is set to private so my profile name and profile picture is the only thing that parents/ carers can access so they do not see my photographs, videos and post content on my social media account.
- I will only communicate with pupils and parents/carers using official academy systems. Any such communication will be professional in tone and manner. These channels of communication are: academy email; approved letters; Academy website; and Academy's text message service (with consent from Head)
- I will not engage in any online activity that may compromise my professional responsibilities.

The academy and the Trust has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the academy:

- I will abide by all relevant guidance and legislation (e.g. Keeping Children Safe in Education / GDPR / AI)
- I will ensure that I am aware of cyber-security risks and that I will not respond to any communications that might put my / academy data or systems at risk from attack
- When using AI systems in my professional role I will use these responsibly and:
    - will only use AI technologies approved by the academy
    - will be aware of the risks of bias and discrimination, critically evaluating the outputs of AI systems for such risks
    - to protect personal and sensitive data, I will ensure that I have explicit authorisation when uploading sensitive academy-related information into AI systems
    - will take care not to infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the learners, being used to train generative AI models without appropriate consent.
    - ensure that documents, emails, presentations, and other outputs influenced by AI include clear labels or notes indicating AI assistance
    - critically evaluate AI-generated outputs to ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing
    - will use generative AI tools responsibly to create authentic and beneficial content, ensuring respect for individuals' identity and well-being
- I will follow the academy's policy on use of mobile phones / devices at the academy and only use them in staff areas or during non-teaching times.
- When I use my personal mobile devices in the academy, (laptops / tablets / mobile phones / USB devices etc) during non-teaching time I will follow the rules set out by the academy in this agreement, in the same way as if I was using academy equipment. I will ensure that any such devices are protected by up to date anti-virus / anti-malware software and are free from viruses.
- When communicating in a professional capacity, I will only use technology and systems sanctioned by the academy.
- I will not use personal email addresses/ accounts on academy ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will exercise informed safe and secure practice when accessing links to content from outside of my organisation to reduce the risk of cyber security threats.
- I will ensure that my data is regularly backed up, in accordance with relevant academy policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not access illegal, inappropriate or harmful content on academy systems.
- I will not bypass any filtering or security systems that are used to prevent access to such content.
- I will not install or attempt to install programmes of any type on an academy device, or store programmes on a computer, nor will I try to alter computer/device settings, unless this is allowed in academy policies / agreed with LA-ICT.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not disable or cause any damage to academy equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the academy Data Security Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that the data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by academy policy to disclose such information to an appropriate authority in line with our legal or contractual obligations.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for academy sanctioned personal use:

- I will ensure that I have appropriate permissions to use the original work of others in my own work and will reflect this with appropriate acknowledgements, particularly where AI has been used to generate content
- Where content is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the academy:

- I understand that this Acceptable Use Policy applies not only to my work and use of academy digital technology equipment on academy site, but also applies to my use of academy systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the academy.
- I will ensure my use of technologies and platforms is in line with the academy's agreed codes of conduct.
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors / Trust / Trustees and in the event of illegal activities the involvement of the Police or termination of employment.

I have read and understand the above and agree to use the academy digital technology systems (both in and out of the academy) and my own devices (in the academy and when carrying out communications related to the academy) within these guidelines.

Signature _____ Date_____

Full Name _____ (printed)

Job title / Role _____

Authorised Signature (Executive Head Teacher/ Head Teacher/Head of School)

I approve this user to be set-up on the academy systems relevant to their role.

Signature _____Date_____

Full Name _____ (printed)

Appendix 4

School Online Safety Incident Report

Date/time of Incident:	
Child and/or Workstation/Device name:	
Incident or concern raised:	
What actions were taken, by whom and why?	
Other information:	
Has any computer or hardware been secured? If so, how/where?	
Has the information been recorded and secured? If so, how/where?	
Member of staff reporting concern:	**Signed:**
Online Safety Coordinator/Designated Safeguarding Lead:	**Signed:**
Action taken by Online Safety Coordinator:	

This record must also be added onto CPOM's.

Appendix 5

Filtering and Monitoring Checklist Register

In line with the DfE filtering and monitoring standards in schools and colleges, this checklist template has been developed as a basis to support schools and colleges in meeting the required standards. Whilst not intended to be exhaustive, this resource can serve as a summary record of checks highlighted within the standards.

Last updated:	**Date:**	**Name/Position:**

Roles and Responsibilities

Role	Responsibility	Name / Position
Responsible Governor	Strategic responsibility for filtering and monitoring and need assurance that the standards are being met.	
Senior Leadership Team Member	Responsible for ensuring these standards are met and: • procuring filtering and monitoring systems • documenting decisions on what is blocked or allowed and why • reviewing the effectiveness of your provision • overseeing reports Ensure that all staff: • understand their role • are appropriately trained • follow policies, processes and procedures • act on reports and concerns	
Designated Safeguarding Lead	Lead responsibility for safeguarding and online safety, which could include overseeing and acting on: • filtering and monitoring reports • safeguarding concerns • checks to filtering and monitoring systems	
IT Service Provider	Technical responsibility for: • maintaining filtering and monitoring systems • providing filtering and monitoring reports • completing actions following concerns or checks to systems	

Professionals Online Safety Helpline
helpline@saferinternet.org.uk
Tel: 0344 381 4772

Reviewing your filtering and monitoring provision

Filtering System	
Filtering Provider and System	
Date Procured	
Date last reviewed	

Monitoring System	
Monitoring Provider and System	
Date Procured	
Date last reviewed	

Review Team [should be conducted by members of the senior leadership team, the Designated Safeguarding Lead (DSL), and the IT service provider and involve the responsible governor]	
Review Date	
Previous Review Date	
Link to last review	

Review Checklist	
the risk profile of your pupils, including their age range, pupils with special educational needs and disability (SEND), pupils with English as an additional language (EAL)	
what your filtering system currently blocks or allows and why	
any outside safeguarding influences, such as county lines	
any relevant safeguarding reports	
the digital resilience of your pupils	
teaching requirements, for example, your RHSE and PSHE curriculum	
the specific use of your chosen technologies, including Bring Your Own Device (BYOD)	
what related safeguarding or technology policies you have in place	
what checks are currently taking place and how resulting actions are handled	

all staff know how to report and record concerns	
filtering and monitoring systems work on new devices and services before release to staff / pupils	
blocklists are reviewed and they can be modified in line with changes to safeguarding risks	

Recommendations / Mitigating Actions

Data Protection Impact Assessment

Schools and colleges that have a technical monitoring system will need to conduct their own Data Protection Impact Assessment (DPIA) and review the privacy notices of third party providers

Link to DPIA	
Conducted by	
Date conducted	

Regular Reports

Type of Report	Filtering / Monitoring
Producer of report	
Recipient of report	
Frequency of report	

Monitoring data is received in a format that your staff can understand	
Users are identifiable to the school / college, so concerns can be traced back to an individual, including guest accounts	

System Checks

Filtering System				
Date checked				
Checks conducted by				
Device	Location	Logged in as	Check Conducted	Result

Confirm your filtering provider is:	
• a member of Internet Watch Foundation (IWF)	
• signed up to Counter Terrorism Internet Referral Unit list (CTIRU)	
• blocking access to illegal content including Child Sexual Abuse Material (CSAM)	

Monitoring System				
Date checked				
Checks conducted by				
Device	Location	Logged in as	Check Conducted	Result

SWGfL© 2023

Appendix 6

Filtering Record sheet

Once per half term, a member of SLT will use a different log in on the website https://testfiltering.com/ to check filtering is installed and working correctly. Screen shots are taken as evidence and stored on the staff drive under the SLT folder, which can only be accessed by SLT.

Date of check	Time of check	Login details	Initials of adult	Signature of adult	Screen shot saved on staff drive	Check okay	Concerns from check	Actions and date completed
9.9.25	4.30pm	St-wanglin-e (teacher login)	EW	Emma Wanglin	✓	✓	/	/

Appendix 7

LIGHTHOUSE MULTI ACADEMY TRUST	**Name**	
	Role	
	AUP review Date	September
	Review Cycle	Annually
	Who reviewed this AUP?	Trust Central Team
	AUP approved by	Trust Board

Acceptable Use Agreement: Governors, Trustees and Members

1. Purpose

This Acceptable Use Policy (AUP) sets out the expectations for Governors, Trustees and Members when accessing, using, and managing academy/trust information, technology, and communication systems.
It's purpose is to ensure:

- Compliance with the law (including GDPR and the Data Protection Act).
- Protection of sensitive information.
- Safe, secure, and ethical use of technology.
- Clear, professional conduct at all times.

This AUP applies to all members, trustees, local governors, co-opted governors, parent governors, associate members, and any other individuals serving in a governance capacity.

2. Scope

The policy covers the use of:

- Academy /trust email accounts and online platforms.
- Documents, data, and information relating to pupils, staff, and governance.
- Personal devices used for governance work (BYOD- bring your own device).
- Communication methods (email, messaging, video calls, online documents).
- Access to academy /trust networks, systems, and cloud services (e.g. GovernorHub, SharePoint, Googledrive).

3. Key Principles

Governors, Trustees and Members must:

- Act professionally, ethically, and in the best interests of the academy/trust.
- Maintain strict confidentiality at all times.
- Use technology safely and responsibly.
- Protect sensitive information and comply with data protection law.

4. Data Protection & Confidentiality

Governors, Trustees and Members must:

- Keep all confidential information secure.
- Only access information necessary for their governance role.
- Not store academy/trust data on personal devices.
- Use academy/trust-approved platforms for storing and viewing documents. (Sharepoint/GovernorHub)
- Avoid downloading documents on personal devices (e.g PC/laptops, I-Pads/Tablets and mobile phones) unless essential and delete them after use.
- Shred or securely dispose of printed papers containing sensitive data.
- Not discuss confidential matters outside authorised meetings.
- Uphold all obligations under **GDPR** and the **Data Protection Act**.

5. Use of Email & Communication Systems

Governors, Trustees and Members must:

- Use the **academy/trust-provided email account** for all governance-related business.
- Avoid using personal email accounts for governor communications.
- Maintain professionalism in all written messages.
- Avoid forwarding confidential or sensitive information to other accounts.
- Not use unsecure messaging apps (e.g., WhatsApp) for confidential governance matters.
- All communication should reflect the dignity, integrity, and professionalism expected of the role.

6. Cybersecurity Expectations

Governors, Trustees and Members must:

- Use strong, unique passwords and change them regularly.
- Enable two-factor authentication where available.
- Lock devices when not in use.
- Ensure personal devices used for governance work have:
    - Up-to-date antivirus software,
    - Operating system updates installed,
    - Secure Wi-Fi connections.
- Not share passwords or login details with others.
- Report any suspected breaches immediately to the **Data Protection Officer (DPO)** and Trust Central Team/CEO.

7. Use of Academy/Trust Systems

Governors, Trustees and Members must not:

- Access staff or pupil records unless explicitly authorised.
- Attempt to gain unauthorised access to systems or files.
- Install software on academy/Trust devices without permission.
- Use academy/Trust systems for personal, commercial, or inappropriate activities.

Note: *Academy/Trust systems include email, MIS (e.g. Arbor), safeguarding systems (e.g. CPOM's), document platforms (e.g. Sharepoint, GovernorHub), and any IT equipment provided.*

8. Remote Meetings & Online Platforms

When joining remote or virtual meetings:

- Use secure platforms approved by the academy/trust *(e.g. Teams)*
- Ensure the environment is private and free from interruption.
- Not record meetings unless authorised by the Chair.
- Store meeting links and documents securely.
- Only use approved Artificial Intelligence (AI) tools to support administrative tasks such as note-taking, transcription, and the drafting of meeting minutes, provided their use complies with data protection, confidentiality, and safeguarding requirements

9. Conduct on Social Media

Governors, Trustees and Members must:

- Not post or share content that could bring the academy or trust into disrepute.
- Not discuss governance matters, staff, pupils, or decisions on social media.
- Follow the academy/trust Social Media Policy.
- Maintain strict political neutrality in public forums when acting in a governance capacity.
- Use social networking sites in accordance with academy policies.
- If following academy/trust accounts (e.g., Facebook, TikTok, Instagram, X), ensure accounts are set to private so that only profile name and picture are visible to parents/carers, avoiding exposure of personal photos, videos, or posts.

10. Use of Personal Devices (BYOD bring your own device**)**
When personal devices (e.g PC/laptops, I-Pads/Tablets and mobile phones) are used for governance work, they must:

- Be password or PIN protected.
- Have encryption enabled where possible.
- Not be shared with others when governance documents are open.
- Be used only to access information via approved secure platforms.
- Have academy/trust documents deleted once no longer needed.
- Report loss or theft of a device immediately.

11. Safeguarding Responsibilities
Governors, Trustees and Members must:

- Complete annual training on:
    - Safeguarding
    - Prevent
    - Data Protection/GDPR
    - Online Safety
    - Cyber Security awareness
- Understand how safeguarding information must be handled and stored.
- Never share safeguarding concerns through insecure methods.
- Follow the academy's/trust's safeguarding procedures at all times.

12. Monitoring & Auditing
The academy or trust may:

- Monitor email activity and access logs where necessary.
- Audit compliance with this AUP.
- Investigate concerns about breaches.
- Monitoring will always be proportionate and in line with legal requirements.

13. Breaches of the Policy
Breaches may include (but are not limited to):

- Loss or unauthorised disclosure of personal data.
- Misuse of email or communication systems.
- Inappropriate use of social media.
- Failure to follow confidentiality requirements.

Consequences may include:

- Withdrawal of access to systems.
- Requirement for further training.
- Reporting to the Chair or Governance Lead.
- Formal action in line with governance regulations.
- Referral to the DPO, ICO, or other authorities in serious cases.

Acknowledgement

All governors, trustees and members must confirm that they have:

- Read and understood this Acceptable Use Policy.
- Agreed to comply with it at all times.

Name: _____ **Role:** _____

Signature: _____ **Date:** _____