Lumen Learning Trust
Learning together for a brighter future

# E-Safety Policy

| | | | |
|---|---|---|---|
| **DATE APPROVED BY LUMEN LEARNING TRUST** | 9th June 2025 | | |
| **REVIEW DATE Biennial** | 9th June 2027 | | |
| **SIGNED EXECUTIVE PRINCIPAL** | Mary Ellen McCarthy  | **DATE** | 9th June 2025 |
| **SIGNED CHAIR OF DIRECTORS** | Jo Roberts  | **DATE** | 9th June 2025 |

Lumen Learning Trust puts the children's needs at the heart of its provision. Our whole school community is committed to enabling the children to become successful lifelong learners and happy, fulfilled adults who can make positive choices about their future.

## 1. Aims

*Lumen Learning Trust aims to:*

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors;
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones');
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

*The 4 key categories of risk*

Our approach to online safety is based on addressing the following categories of risk:

- *Content* – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism;
- *Contact* – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes;
- *Conduct* – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying;
- *Commerce* – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

## 2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

This policy complies with our funding agreement and articles of association.

## 3. Roles and responsibilities

*3.1 The Board of Directors*

The Trust's Board of Directors has overall responsibility for monitoring this policy and holding school headteachers to account for its implementation.

They will:

- Co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).
- Ensure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.
- Ensure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

- Ensure children are taught how to keep themselves and others safe, including keeping safe online.
- Ensure all trust schools have appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness.
- Review the DfE's filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:
    - Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
    - Reviewing filtering and monitoring provisions at least annually;
    - Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
    - Having effective monitoring strategies in place that meet their safeguarding needs.

All Directors will:

- Ensure that they have read and understood this policy;
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet;
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school approach to safeguarding and related policies and/or procedures;
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

*3.2 The headteacher*

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

*3.3 The designated safeguarding lead*

Details of the school's designated safeguarding lead (DSL) and deputies are set out in each school's individual child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school;
- Working with the headteacher and other staff, as necessary, to address any online safety issues or incidents;
- Responding to safeguarding concerns identified by filtering and monitoring.
- Managing all online safety issues and incidents in line with the school child protection policy;
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy;
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour 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 school to the headteacher and/or governing board.
- Undertaking annual risk assessments that consider and reflect the risks children face.
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively.

This list is not intended to be exhaustive.

*3.4 The Trust Central Team*

Members of the central Trust support function have delegated responsibility to ensure this policy is adhered to, in particular:

- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks.
- Devising and rolling out efficient processes to allow the school DSL to respond to safeguarding concerns identified by filtering and monitoring.

- Providing Directors with assurance that filtering and monitoring systems are working effectively and reviewed regularly.

*3.5 The ICT support function*
The ICT support function is responsible for:
- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material;
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly;
- Conducting a full security check and monitoring the school's ICT systems on an annual basis;
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files;

This list is not intended to be exhaustive.

*3.6 All staff and volunteers*
All staff, including contractors and agency staff, and volunteers are responsible for:
- Maintaining an understanding of this policy;
- Implementing this policy consistently;
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use;
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by adding an incident to the school's CPOMS database.
- Following the correct procedures by emailing their request to the DSL if they need to bypass the filtering and monitoring systems for educational purposes.
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy;
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy;
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'.

This list is not intended to be exhaustive.

*3.7 Parents*
Parents are expected to:
- Notify a member of staff or the headteacher of any concerns or queries regarding this policy;
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet;
- Parents can seek further guidance on keeping children safe online from the following organisations and websites:
    - 
    - What are the issues? – UK Safer Internet Centre
    - Online safety topics for parents/carers – Childnet
    - Parent resource sheet – Childnet

*3.8 Visitors and members of the community*
Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

## 4. Educating pupils about online safety

*The Internet and digital communications are important:*
- The Internet is an essential element in 21st century life for education, business and social interaction;

- Each school within the Trust has a duty to provide pupils with quality Internet access as part of their learning experience;
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils;
- School Internet access is provided by Talk Straight and includes filtering appropriate to the age of pupils;
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use;
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation;
- Pupils will be shown how to publish and present information appropriately to a wider audience.

*Pupils will be taught how to evaluate Internet content:*

- The school will seek to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law;
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy;
- Pupils will be taught how to take care of their own safety and security as well as how to report unpleasant Internet content e.g. using the CEOP Report Abuse icon or Hector Protector, through E-Safety being delivered half-termly.

Pupils will be taught about online safety as part of the curriculum.

In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private;
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Pupils in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly;
- Recognise acceptable and unacceptable behaviour;
- Identify a range of ways to report concerns about content and contact;
- Be discerning in evaluating digital content.

By the end of primary school, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not;
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous;
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them;
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met;
- How information and data is shared and used online;
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context);
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know;
- The benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing
- How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private
- Where and how to report concerns and get support with issues online

The safe use of social media and the internet will also be covered in other subjects where relevant. Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

## 5. Educating parents and carers about online safety

Each school will raise parent and carer awareness of internet safety in letters or other communications home, and in information via our website and our social media accounts.

This policy will also be shared with parents and carers. Online safety will also be covered during parents' evenings.

If parents or carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the school headteacher.

## 6. Cyber-bullying

*6.1 Definition*
Cyber-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 1 person or group by another person or group, where the relationship involves an imbalance of power.

*6.2 Preventing and addressing cyber-bullying*
To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

Our schools will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their classes.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All school staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

Our schools also send information 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 a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

*6.3 Examining electronic devices*
The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence.

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher;
- Attempt to make contact with the pupil's parent to discuss the concern and why a search is necessary. They must attempt to seek the parent's cooperation however it is understood that the search can go ahead without parental permission

- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it;
- Seek the pupil's cooperation.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence.

If inappropriate material is found on the device, it is up to the headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

In the event of inappropriate material being found, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members should:

- Photograph the content and upload it to CPOMS. Once uploaded to CPOMS the photograph must be deleted from the device that was used to capture the image;
- Inform the pupil's parent of the content;
- Request the pupil and the parent delete the content.

Following the incident, the pupil and the parent must meet with the headteacher or a senior leader authorised by the headteacher to review the incident in the context of the Family Acceptable Use of ICT Agreement and E-Safety rules. The pupil and the parent will be required to sign a new copy of this agreement.

If the headteacher and any pupil who has been harmed by the incident agree this as a way forward, there may be a restorative conversation with those involved, in line with the Behaviour Management Policy.

If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- Not view the image;
- Confiscate the device and report the incident to the Headteacher as Designated Safeguarding Lead for the school immediately, who will decide what to do next. The Headteacher will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation;
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people;
- Our behaviour management policy.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

## 7. Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

Lumen Learning Trust recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

We will will treat any use of AI to bully pupils very seriously, in line with our behaviour management policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school/trust, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by it, including, but not limited to, pupils and staff.

Any use of Artificial Intelligence should be carried out in accordance with our AI usage policy.

**8. Acceptable use of the internet in school**
All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

**9. Pupils using mobile devices in school**
Pupils are able to bring mobile devices to school but they must be handed to an adult as they enter the school building at the start of the day. Mobile devices will be stored securely in the school office during the school day and handed back to the pupil at afternoon dismissal.

Any breach of these arrangements by a pupil will result in the confiscation of their device.

**10. Staff using work devices outside school**
All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol);
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device;
- Making sure the device locks if left inactive for a period of time;
- Not sharing the device among family or friends;
- Installing anti-virus and anti-spyware software;
- Keeping operating systems up to date by always installing the latest updates;
- Staff members must not use the device in any way which would violate the school's terms of acceptable use;
- Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from their school's IT support provider.

**11. Managing Internet Access**

*Information system security*

- The school will use a recognized internet service provider or regional broadband consortium;
- School computing systems security will be reviewed regularly, ensuring internet access has age appropriate filtering;
- Virus and anti-spam protection will be updated regularly;
- Security strategies will be discussed with the Local Authority;
- Password convention will require upper and lower case letters, symbols and numbers to be used to ensure any password is at least 'Strong'.

*E-mail*

- Pupils and staff may only use approved e-mail accounts on the school system. For pupils, e-mail access is via a generic class e-mail account. No individual personalised e-mail accounts will be created for pupils;
- Pupils must immediately tell a teacher if they receive an offensive e-mail;
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission;
- Staff to pupil email communication must only take place via the child's parent/carer to the school's office email address and will be monitored;
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known;
- The school will consider how e-mail from pupils and staff to external bodies is presented and controlled;
- The forwarding of chain letters is not permitted.

*Published content and the school website*

- The contact details on each school website are the school address, e-mail and telephone number. Staff or pupil personal information will not be published;
- The Head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate;
- The school websites should comply with and respect copyright law.

*Publishing pupil's images and work*

- Photographs that include pupils will be selected carefully, wherever possible reflecting the children's learning or general school life in content;
- The school will include images of children from different ethnic backgrounds in our communications wherever possible, and include positive images of children with disabilities to promote our school as an inclusive community, and to comply with the Disability Discrimination Act;
- Pupils' full names will be avoided on the school Websites or learning platform, as appropriate, including in blogs, forums or wikis, particularly in association with photographs;
- When their child starts at a Lumen school parents and carers will be asked to provide written consent for their child's image to be published on the school website, social media and external media such as press publications. This will be kept on each pupil's file. Parents and carers are given the opportunity to review their consents again at the start of Key Stage 2. Consent can be freely changed whenever a parent and carer chooses although it should be noted that retrospective changes cannot be made;
- Images of pupils will only be taken on school devices such as digital camera or class iPad;
- The storage of pupil images will be within the secure school server or secure whole school storage account (e.g. Google Drive, Dropbox) accessible by strong password only. Storage should never be via personal storage accounts;
- Parents and carers are able to take photographs or video for their own personal use when attending a school event only if agreed by the Headteacher in advance of the event. However, use of the images taken/recorded must not be uploaded to the internet or social media if any other children other than their own is also visible;
- The school will annually invite an official photographer into school to take portraits/photographs of individual children and/or class groups. These will be for parent/carer use only.

*Social networking*

- The school will control access to social networking sites, and consider how to educate pupils in their safe use e.g. use of passwords;
- Newsgroups will be blocked unless a specific use is approved;
- Pupils will be advised never to give out personal details of any kind which may identify them or their location;
- Pupils and parents/carers will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils;
- Staff will be made aware of the Lumen Social Media for School Staff policy and Social Media for Schools policy for appropriate professionalism with regards to social networking;
- Parents and pupils will be advised that photos or videos taken by them within school should not be uploaded to any social network site and the affected school has permission to ask for these to be removed;

- Pupils will also be advised not to place personal photos on any social network space. They should consider how the public the information is and consider using private areas. Advice will be given regarding the background detail which could identify a pupil or their location e.g. house number, street name or school;
- Pupils will be advised about how to communicate with peers appropriately (including the use of gaming forums as well as social networks). Staff and parents will be encouraged to cultivate an atmosphere of 'telling' and respond to reports of Cyber-bullying following the Trust's anti-bullying policy;
- Staff will be advised that social media networking sites should not be used to discuss work or school related topics;
- Staff will be advised that on sites such as Facebook, they should consider very carefully if they are friends with parents regardless of their relationship with the parent outside of the school environment. Staff who are also parents at a Lumen school should use their professional judgement and should choose which group to be friends with – ideally parents or staff, not both;
- Please refer to the Lumen Learning Trust policies on Social Networking for more information.

*Use of personal devices*

- Personal equipment may be used by staff to access school IT systems provided their use complies with the Lumen Learning Trust staff 'ICT User Agreement' and 'Email Security & Etiquette Guidance';
- Staff must never use a personal device to capture a pupil's image;
- Any images subsequently stored should be held in a secure location within their school's network, ideally in a shared folder with access reviewed frequently and at least annually;
- The Trust and its schools cannot be held responsible for the loss or damage of any personal devices used in school or for school business.

*Managing filtering*

- The school will work in partnership with a chosen provider to ensure systems to protect pupils are reviewed and improved;
- Strategies to ensure safe online behaviour and responsible use of new technologies for both staff and pupils is in place at all Lumen schools through the use of continuous monitored filtering software;
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the E-safety Lead/Computing Lead or DSL;
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. This will include random checks of white/black lists. Any inappropriate content should be reported to the E-safety Lead/Computing Lead, DSL and IT support provider;
- Password integrity for filtering will be monitored by the E safety Lead/Computing Lead and DSL.

*Managing videoconferencing*

- Videoconferencing will use the educational broadband network to ensure quality of service and security rather than the Internet;
- Videoconferencing should take place via the school's preferred provider Google Meet wherever possible in the first instance however Microsoft Teams and Zoom will be made available for staff if required;
- Videoconferencing will be appropriately supervised for the pupils' age;
- Controls are in place to ensure that only staff members have the ability to create a videoconference session or to record a session.

*Managing emerging technologies*

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is permitted;
- Staff and pupil personal mobile phones and associated cameras will not be used within the school environment except as part of an educational activity;
- The sending of abusive or inappropriate text messages is forbidden;
- Staff will use a Trust or school owned telephone in all instances where contact with a parent or carer is required. If for whatever reason this is not possible, a personal device can be used but only via the CallSwitch app.

*Protecting personal data*

- Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation 2018. Further details can be found in our Privacy Notices.

## 12. Policy Decisions

*Authorising Internet access*

- All staff must read and sign the Lumen Learning Trust 'ICT User Agreement' and 'Email Security & Etiquette Guidance' documents before using any school computing resource;
- Each school will maintain a current record of all their staff and pupils who are granted access to school computer systems;
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials;
- At Key Stage 2, access to the Internet will be with teacher permission with increasing levels of autonomy;
- Parents will be asked to sign and return the 'Lumen Learning Trust Family Acceptable Use of ICT Agreement and E-Safety Rules';
- Pupils will be asked to sign an acceptable use of the internet form prior to using the internet as part of their E-Safety learning;
- Any person not directly employed by the school (e.g. school governors) will be asked to sign an 'ICT User Agreement' and 'Email Security & Etiquette Guidance' document before being allowed to access to Trust computer systems.

*Assessing risks*

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Lumen Learning Trust cannot accept liability for the material accessed, or any consequences of Internet access;
- The school will audit computer use to establish if the E-safety policy is adequate and that the implementation of the E-safety policy is appropriate and effective;
- The school will log any computing related concerns on their E-Safety log, which will be monitored by the Computing Lead.

*Handling E-safety complaints*

- Complaints of Internet misuse will be dealt with by a senior member of staff;
- Any complaint about staff misuse must be referred to the applicable Head teacher;
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures;
- Pupils and parents will be informed of the complaints procedure;
- Pupils and parents will be informed of consequences for pupils misusing the Internet via the Family Acceptable Use Agreement.

*Community use of the Internet*

- All use of the school Internet connection by the community and other organisations shall be in accordance with the school E-safety policy.

## 13. Communications Policy

*Introducing the E-safety policy to pupils*

- Appropriate elements of the E-safety policy will be shared with pupils;
- E-safety rules will be posted in all networked rooms to remind students when using any form of technology;
- Pupils will be informed that network and Internet use will be monitored and individual pupils spoken to about their use if necessary;
- Curriculum opportunities to gain awareness of E-safety issues and how best to deal with them will be provided for pupils.

*Staff and the E-safety policy*

- All staff will be given this E-safety Policy and its importance explained.
- Staff should be aware that Internet traffic is monitored and traced to the individual user. Discretion and professional conduct is essential;
- Staff that manage filtering systems or monitor computer use will be members of the Trust and individual school senior leadership teams as stipulated by the Headteacher and will have clear procedures for reporting issues.

*Enlisting parents' support*

- Parent and carer attention will be drawn to this E-safety Policy in newsletters and on the school website;
- Parents and carers will from time to time be provided with additional information on E-safety;
- The school will ask all new parents and carers to sign the 'Lumen Learning Trust Family Acceptable Use of ICT Agreement and E-Safety Rules' when they register their child with the school;
- Internet issues will be handled sensitively and parents will be advised accordingly.

## 14. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and the LLT Family acceptable use of ICT agreement and e-safety rules. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the relevant staff policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident. The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

## 15. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse;
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages;
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups;
    - Sharing of abusive images and pornography, to those who don't want to receive such content;
    - Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse;
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks;
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term.

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

All pupils will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Pupils will also receive age-appropriate training on safeguarding issues such as cyberbullying and the risks of online radicalisation.

**16. Monitoring arrangements**

The DSL and deputies log behaviour and safeguarding issues related to online safety via the school's electronic pastoral reporting tool.

This policy will be reviewed biennially by senior leaders. At every review, the policy will be shared with the Board of Directors.

**17. Links with other policies**

This online safety policy is linked to our:

- Anti-Bullying Policy
- Behaviour Management Policy
- Child Protection Policy
- Family Acceptable Use of ICT Agreement and E-Safety Rules
- ICT User Agreement for staff
- Email security and etiquette guidelines for staff
- Parent and Visitor Code of Conduct
- Social Media and Networking for School Use Policy
- Social Media for School Staff Policy
- School Development Plan
- Staff Code of Conduct