Lumen Learning Trust

Learning together for a brighter future

E-safety Policy

DATE APPROVED BY LUMEN LEARNING TRUST	15th March 2019		
REVIEW DATE Biennial	15th March 2020		
SIGNED DEPUTY EXECUTIVE PRINCIPAL	Sarah Kober SKober	**DATE**	15th March 2019
SIGNED CHAIR OF DIRECTORS	Ray Vango	**DATE**	15th March 2019

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.

The E-safety Policy is part of the School Development Plan and relates to other policies including those for Computing, Bullying and for Child Protection.

Our E-safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by the Senior Leadership Team and approved by governors.

The E-safety Policy and its implementation will be reviewed annually.

Teaching and learning

Why 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 students 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.
- The school Internet access is provided by RM 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.

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 a school 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 the 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. 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 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 Computing Code of Conduct for appropriate professionalism with regards to social networking.
- Parents and pupils will be advised that photos or videos taken 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 not be 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 – parents or staff, not both.
- Please refer to the Lumen Learning Trust policy 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 'ICT User Agreement' and 'Email Security & Etiquette Guidance'.
- Staff must never use a personal device to capture a pupil's image.
- The Trust and it's 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 Surrey County Council 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.
- 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 and IT support provider.
- Password integrity for filtering will be monitored by the E safety Lead/Computing Lead.

Managing videoconferencing

- Videoconferencing will use the educational broadband network to ensure quality of service and security rather than the Internet.
- Videoconferencing will be appropriately supervised for the pupils' age.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- 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 school telephone in all instances where contact with a parent or carer is required.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation 2018.

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 'Pupil & Family E-Safety Acceptable Use Policy'.

- 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 the Internet from the school site.

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. Neither the school nor Surrey County Council can 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 Acceptable Use policy.

Community use of the Internet

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

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 the School 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 a school senior leadership team as stipulated by the Headteacher and will have clear procedures for reporting issues.

Enlisting parents' support

- Parents' and carers attention will be drawn to the School 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 to sign the 'Pupil & Family E-Safety Acceptable Use Policy' when they register their child with the school.
- Internet issues will be handled sensitively and parents will be advised accordingly.