ESTABLISHED 1906

Lord's Independent School

E-Safety POLICY

Review Schedule: Annual

Lord’s Independent School

E-Safety Policy

Next review date: August 2025

Introduction

The school aims to ensure that every student in its care is safe, and the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods but also pose more significant and more subtle risks to young people. Our students are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking, abuse, and radicalisation.

New technologies are continually enhancing communication, the sharing of information, learning, social interaction, and leisure activities. Current and emerging technologies used in and outside of school may include:

- Websites.
- Email and instant messaging.
- Blogs.
- Social networking sites.
- Chat rooms.
- Artificial intelligence (AI).
- Metaverse.
- Music/video downloads.
- Gaming sites.
- Text messaging and picture messaging.
- Video calls.
- Podcasting.
- Online communities via games consoles; and
- Mobile internet devices such as smartphones and tablets.

This policy is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements.

While exciting and beneficial both in and out of the context of education, much IT, particularly online resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies.

The school is aware of the issues within the realms of E-Safety are considerable, and these can be broadly categorised into four areas of risk:

- **content:** being exposed to illegal, inappropriate, or harmful content, for example, pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- **contact:** being subjected to harmful online interaction with other users; for example, 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:** online behaviour that increases the likelihood of, or causes, harm; for example, making, sending, and receiving explicit images (e.g., consensual, and nonconsensual 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. If you feel your students, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

We understand the responsibility to educate our students on E-Safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and

related technologies in and beyond the classroom. We also understand the importance of involving students in discussions about E-Safety and listening to their fears and anxieties as well as their thoughts and ideas.

This policy applies to all members of the school community, including staff, students, parents, and visitors, who have access to and are users of the school IT systems and equipment. In this policy 'staff' includes teaching and nonteaching staff, governors, and volunteers. 'Parents include students' carers and guardians. 'Visitors' includes anyone else who comes to the school, including occasional volunteers.

Both this policy and the Acceptable Use Agreements cover:

- IT equipment and mobile devices provided by the school to members of teaching and non-teaching staff, e.g., laptops, monitors, phone systems, dongles.
- Personal IT equipment/devices owned and used by students and guest speakers at the school to access our platform.

Please note that, as outlined below, staff should not be using personal equipment/devices to access school platforms.

Roles & Responsibilities

Headteacher and the Senior Leadership Team

This group is responsible for the approval of this policy and for reviewing its effectiveness. The Headteacher is responsible for the safety of the members of the school community, and this includes responsibility for E-Safety. The Headteacher has delegated day-to-day responsibility to the Designated Safeguarding Lead (DSL). In particular, the role of the Headteacher and the Senior Leadership team is to ensure that staff are adequately trained about E-Safety and are aware of the school procedures and policies that should be followed in the event of the abuse or suspected breach of E-Safety in connection to the school.

Designated Safeguarding Lead (DSL)

The School's DSL is responsible to the Headteacher for the day-to-day issues relating to E-Safety. The DSL has the responsibility for ensuring this policy is upheld by all members of the school community and works with IT staff to achieve this. They will keep up to date on current E-Safety issues and guidance issued by relevant organisations.

IT staff

The school's technical staff have a key role in maintaining a safe technical infrastructure at the school and in keeping abreast of the rapid succession of technical developments. They are responsible for the security of the school's systems, its data and for training the school's teaching and administrative staff in the use of IT. They monitor the use of the internet and emails, maintain content filters, and report inappropriate use to the DSL and Executive Headteacher.

Teaching and support staff

As with all issues of safety at this school, staff are encouraged to create a talking and listening culture to address any E-Safety issues which may arise in classrooms daily.

Students

Students are responsible for using the school IT systems responsibly, and for letting staff know if they see IT systems being misused.

Parents and Carers

The school believes that it is essential for parents to be fully involved in promoting E-Safety both in and outside of school. We regularly consult and discuss E-Safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage. The school will always contact parents if it has any concerns about students' behaviour in this area and likewise, it hopes that parents will feel able to share any concerns with the school.

Education and Training

Staff: awareness and training

New teaching staff receive information on E-Safety as part of their induction.

All teaching staff receive regular information and training on E-Safety issues in the form of INSET training and internal meeting times and are made aware of their responsibilities relating to the safeguarding of children within the context of E-Safety.

All staff working with children are responsible for demonstrating, promoting, and supporting safe behaviours in their classrooms and following school E-Safety procedures.

Teaching staff are encouraged to incorporate E-Safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community.

A record of concern must be sent by staff as soon as possible if any incident relating to E-Safety occurs and be provided directly to the school's DSL. The School's DSL keeps a log of any reported incidents and follows up through appropriate communication with students, parents, or staff, monitoring as necessary.

Students: E-Safety in the curriculum

We believe it is essential for E-Safety guidance to be given to students on a regular and meaningful basis. We continually look for new opportunities to promote E-Safety and regularly monitor and assess our students' understanding of it.

The school provides opportunities to teach about E-Safety within a range of curriculum areas. Educating students on the dangers of technologies that may be encountered outside school will also be carried out via PSHE, as well as informally when opportunities arise.

At age-appropriate levels, and usually, via PSHE, students are taught about their E-Safety responsibilities and to look after their online safety. Students are taught about recognising online sexual exploitation, stalking and grooming, the risks, and their duty to report any such instances they or their peers come across. Students can report concerns to the Designated Safeguarding Lead or any member of staff at the school, who will then report concerns to the DSL.

Students are also taught about relevant laws applicable to using the internet, such as data protection and intellectual property. Students are taught about respecting other people's information and images through discussion and classroom activities.

Students should be aware of the impact of cyberbullying and know how to seek help if they are affected by these issues. Students should approach the Designated Safeguarding Lead as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.

Parents

The school seeks to work closely with parents and guardians in promoting a culture of E-Safety. The school will always contact parents if it has any concerns about students' behaviour in this area and likewise, it hopes that parents will feel able to share any concerns with the school.

The school recognises that not all parents and guardians may feel equipped to protect their son or daughter when they use electronic equipment at home and would encourage parents to seek advice via our Customer Support team at any time.

Use of school and personal devices

Staff

School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. Staff should only use the school device that is allocated to them for schoolwork. When they are not using a device staff should ensure that it is locked to prevent unauthorised access.

Staff should ensure that they do not use personal electronic devices (e.g., non-school-owned laptops, mobile phones) for work purposes.

Personal telephone numbers, email addresses, or other contact details may not be shared with students or parents/carers and under no circumstances may staff contact a student or parent/carer using a personal telephone number, email address, social media, or other messaging systems.

Staff must not send school information to their personal devices/ personal email accounts. If in any doubt a device user should seek clarification and permission from the school's IT team before attempting to gain access to a system for the first time. Users must follow the written procedures for connecting to the school systems.

Students, Parents and Carers

Students will access our school platform via personal devices, which may include PCs, laptops, and mobile devices. Students and their families are responsible for the safe and appropriate use of these devices, including security.

It is highly recommended that anti-virus software is installed and that parents set up privacy settings/ content blocks to ensure that their children cannot access inappropriate content. Our IT team can provide technical support remotely, but only in relation to our school systems.

It is highly recommended that parents monitor students' use of electronic devices, particularly during the school day.

The school asks that students do not use other devices, other than those directed to, during lessons. The school recognises that personal mobile devices are sometimes used by students for medical purposes or as an adjustment to assist students who have disabilities or special educational needs. Where a student needs to use a mobile device for such purposes, the student's parents or carers may wish to inform the school so that the student's teachers and other relevant members of staff will be informed.

Communication- Email, Messaging, social media

Staff

Staff must not access social networking sites, personal email or any website or personal email which is unconnected with schoolwork or business from school devices or while teaching / in front of students. Such access may only be made from staff members' personal devices.

When accessed from staff members' personal devices, staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of the school.

The school has taken all reasonable steps to ensure that the school platform is safe and secure. Staff should be aware that all communications through the school platform and staff email addresses are monitored.

Staff must immediately report to the DSL and IT Service Desk the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to the IT Service Desk.

Any online communications, both in and out of school, on school or personal devices, must not either knowingly or recklessly:

- place a child or young person at risk of harm or cause actual harm.
- bring the school into disrepute.
- breach confidentiality.
- breach copyright.
- breach data protection legislation: or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
    - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age.
    - using social media to bully another individual; or
    - posting links to or endorsing material which is discriminatory or offensive.

Under no circumstances should school students or parents be added to staff social network 'friends' or contacted through social media.

Any digital communication between staff and students or parents/carers must be professional in tone and content. Under no circumstances may staff use their personal email address, mobile or landline phone number or social media, to contact a student or parent/carer. The school ensures that staff always have access to their work email address, for use as necessary on school business.

Students

All students are issued with their personal school email addresses for use on our platform and by remote access. Access is via a personal login, which is password-protected. This official email service may be regarded as safe and secure and must be used for all schoolwork, including communication with teachers, non-teaching staff and students. Students should be aware that all communications through the school platform and school email addresses are monitored.

Our IT staff work hard to ensure our platform is safe and secure. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for schoolwork/research purposes, students should contact IT through Live Technical Support for assistance.

Students must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such communication, to the DSL / IT Service Desk / or another member of staff.

When using social media accounts, the school expects students to think carefully before they post any information online or repost or endorse content created by other people. Content posted should not be able to be deemed inappropriate or offensive, or likely to cause embarrassment to the individual or others. This includes content of a sexual nature and content that is offensive or discriminatory.

Students must report any accidental access to materials of a violent or sexual nature directly to the DSL / IT through a member of staff. Deliberate access to any inappropriate materials by a student will lead to the incident being recorded on their file and will be dealt with under the school's Behaviour Policy.

Students should be aware that the storage/sharing/sending of abusive or inappropriate messages or content via their personal devices, even outside of the school platform, is considered a breach of the school's Behaviour Policy. Concerns will be passed to the DSL, who will investigate further and may also refer the matter to the relevant Local Authority's Designated Officer (LADO) or police.

Camera Expectations

We expect that all teachers will use webcams when delivering lessons online, and we also facilitate students using webcams during lessons. We have found that there are many benefits for students using webcams during lessons:

- Students feel a greater sense of community.
- Teachers can interpret visual cues, e.g., recognising when a student is 'stuck' and needs help.
- Students can quickly show the work they have completed, and teachers can give feedback or address misconceptions during the live lesson, rather than waiting to see an uploaded assignment.
- To keep all our students safe, all teachers and students using webcams during lessons are required to adhere to our user guidelines.
- Users should be dressed appropriately - for instance, the following clothing would be inappropriate and may result in students being removed from the classroom: pyjamas, clothing with offensive language, images or logos, vest-tops, and see-through clothing.
- Users should consider the webcam background, e.g., wall displays and items behind them that will be visible to others. Filters are not recommended, but where possible, users should be working in a quiet, uncluttered environment. Posters or decor with offensive language or images should not be visible.
- Other people should not be visible on the webcam during lessons, e.g., parents or siblings.
- The school will ensure that lesson recordings are only available to students enrolled in that particular class, their teachers, and our safeguarding team.
- All Live Lessons are recorded and held in a secure location in case they need to be reviewed for academic or safeguarding purposes.
- Computers and laptops will be in an appropriate location, avoiding bedrooms for example.
- Language will be appropriate and professional, including any family members/friends in the background.
- When you are not talking, ensure that your microphone is muted.
- Avoid talking over other students where possible. If you want to contribute to the discussion, then use the 'raise hand' function and wait for the teacher to call upon you or a natural break in the conversation.

We know that many students, like more interaction with their friends, peers, and classmates through camera and mic use. We do also know however that some students strongly value the choice to use text only – either due to their specific needs or because they benefit from a distraction and anxiety-free experience. We wish to meet all needs and deliver a personalised learning experience that gives every student the perfect learning environment for them.

Our approach is to offer clear choices about what type of communication tools in lessons will best suit your child and to inform parents if these tools are being used by your child in their lessons. In this way, we can provide an experience for each student that meets their needs and engages and excites them.

To give parents flexibility, we have the following contribution levels that can be set as a global setting for their child's lessons (please note the default setting for students unless adjusted by parents is Level 3):

1. Contribute by text chat, collaborating by writing on shared documents and whiteboards, and sharing my work.
2. Contribute by text chat, collaborating on shared documents and whiteboards, by sharing my work, and on mic.
3. Contribute by text chat, collaborating on shared documents and whiteboards, by sharing my work, on mic, and on camera.

Course of action if inappropriate content is found

- If inappropriate web content is found (i.e., that is pornographic, violent, sexist, racist or horrific) the user should:
  - Turn off the monitor or minimise the window.
  - Report the incident to their teacher, if a student, or other responsible adult, or to the DSL.

- The teacher/responsible adult should:
  - Ensure the well-being of the student.
  - Note the details of the incident, especially the web page address that was unsuitable (without reshowing the page to the students).
  - Report the details of the incident to the DSL.

- The DSL will then:
  - Log the incident and take any appropriate action.
  - Where necessary report the incident to parents and/or the IT team so that additional actions can be taken.

Filtering and Monitoring

Students at Lord's access lessons from home and school, respectively. Where students are accessing lessons from home, there is limited ability of staff members to prevent students from accessing websites that the school does not deem appropriate for children and young people. We rely on the cooperation of parents and carers to monitor the online activity of their child or young person. Where students are attending their lessons from a school building.

The school will use websites, applications and programmes that are appropriate to the age and experience of Students. The school recommends that this should continue into the home when utilising technologies and the internet outside of school time. Filtering and monitoring of children and young people's online activity is strongly recommended to parents, carers, and families.

Staff and Students who discover that an unsuitable site has been shared or posted on school platforms must be reported to a member of senior leadership.

The school will report any online material it believes to be illegal to the appropriate agencies i.e., IWF or Child Exploitation and Online Protection command (CEOP).

The school recognises the existence of the Internet Watch Foundation list and would encourage parents and carers to ensure their child or young person is not accessing the sites mentioned.

Parents and carers will be informed of any breaches of behaviour, safeguarding, anti-bullying, and E-Safety policies involving their child or young person.

The school is aware that students, parents, and carers cannot rely on filtering and monitoring alone to safeguard students; effective classroom management and regular education about safe and responsible use are essential.

To support schools and colleges to meet this duty, the Department for Education has published filtering and monitoring standards which set out that schools and colleges should:

- identify and assign roles and responsibilities to manage filtering and monitoring systems.
- review filtering and monitoring provisions at least annually
- block harmful and inappropriate content without unreasonably impacting teaching and learning.
- have effective monitoring strategies in place that meet their safeguarding needs.

We will review the standards and discuss with IT staff and service providers what more needs to be done to support these standards.

Data storage and processing

The school takes its compliance with the Data Protection Act 2018 seriously. Please refer to the Data Protection Policy and the Acceptable Use agreements for further details.

Staff are expected to save all documents, presentations and data relating to their work to the school platform- e.g., Student Drive / G Drive as directed by the teaching staff.

Staff devices should be encrypted if any data or passwords are stored on them.

The school does not endorse the use of other types of data storage, e.g., USB memory sticks, CDs, or portable drives, except in the case of coursework submitted for GCSE, and this is subject to approval by the IT team. No personal data of staff or students should be stored on personal memory sticks, CDs, or portable drives.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the IT Service Desk

Password security

Students and staff have individual school logins. Staff and students are regularly reminded of the need for password security.

All students and members of staff should:

- use a strong password (usually containing eight characters or more and containing upper- and lower-case letters as well as numbers), which should be changed every three months.
- not write passwords down.
- not share passwords with other students or staff; and

Safe use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking, or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their images on the internet (e.g., on social networking sites).

Parents/carers and students are not permitted to record or create images of any part of the school platform, including lessons. To respect everyone's privacy and for the protection of data, recordings and images should not be published on blogs or social networking sites etc.

Students must not take, use, share, publish or distribute images of others.

Staff may need to record or create digital images to support educational aims but must follow this policy and the Acceptable Use Policy concerning the sharing, distribution, and publication of those videos/images. Those images should only be taken on school equipment: personal equipment should not be used for such purposes.

Written permission from parents or carers will be obtained before photographs of students are published on the school website, see Parent Contract for more information. Photographs published on the school website, or displayed elsewhere, that include students, will be selected carefully, and will comply with good practice guidance on the use of such images.

Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Misuse

The school will not tolerate illegal activities or activities that are inappropriate in a school context and will report illegal activity to the police and other relevant agencies or enforcing authorities. If the school discovers that a child or young person is at risk as a consequence of online activity, it may seek external assistance. This includes but is not limited to, involvement in cyberbullying, 'sexting' or sharing youth-produced sexual images, involvement in radicalisation, grooming and other high-risk activities.

Incidents of misuse or suspected misuse must be dealt with by staff following the school's policies and procedures detailed in the Safeguarding Policy.

The school will impose a range of sanctions on any student who misuses technology to bully, harass or abuse another student. Our school's Behaviour Policy has additional information on these issues.

Electronic Devices - search and deletion

Schools now have the authority to 'delete data' stored on student's electronic devices. In our school, this is only likely to occur when the IT Technical support team are working remotely to support the student in their access to our school platform.

If a member of staff finds a pornographic image (e.g., either a member of the IT Technical support team or a member of teaching staff during a lesson, if the student is screen-sharing), they should immediately bring this to the attention of the DSL or the Headteacher, who will investigate further.

Images found on a mobile phone or other electronic devices can be deleted unless it is necessary to pass them to the police. The member of staff must have regard to the local regulations and guidelines when determining what is a "good reason" for examining or erasing the contents of an electronic device. In determining a 'good reason' to examine or erase the data or files, the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, disrupt teaching, or break the school rules.

If inappropriate material is found on the device the member of staff must consult with the DSL or one of the Heads of School to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police.

All school staff should be aware that behaviours linked to sexting put a child in danger. The school's Senior Leadership Team should ensure sexting and the school's approach to it is reflected in the child protection policy.

Loading/installing software.

For this policy, software relates to all programs, images, or screensavers, which can be downloaded or installed from other media:

- Any software loaded onto the school system or individual computers and laptops/devices must be properly licensed and free of viruses.
- Only authorised persons, such as the IT team may load software onto the school platform or individual school owned computers.
- Where staff are authorised to download software to their laptops/devices, they must ensure that this is consistent with their professional role and that they are satisfied that any downloaded images and video clips do not breach copyright.

Compliance, Sanctions and Disciplinary Matters

Non-compliance with this policy exposes the school to risks. If a breach of this policy occurs, the school will respond immediately by issuing a verbal and then written warning to the staff member, student, or parent. Guidance will also be offered.

If steps are not taken by the individual to rectify the situation and adhere to the policy, then the user's access to our platform may be temporarily withdrawn.

For persistent breaches of this policy, the school will permanently revoke permission to access school platforms.

Acceptable Use Policy

This policy applies to all members of the school community, including staff, students, parents, and visitors. In this policy 'staff' includes teaching and non-teaching staff, governors, and regular volunteers. 'Parents' includes students' carers and guardians. 'Visitors' includes anyone else who comes to the school, including occasional volunteers.

Online Behaviour

As a member of the school community, you should follow these principles in all of your online activities:

- Ensure that your online communications, and any content you share online, are respectful of others.
- Do not access, create, or share content that is illegal, deceptive, or likely to offend other members of the school community (for example, material that is obscene, or promotes violence, discrimination, or extremism).
- Respect the privacy of others. Do not share photos, videos, contact details, or other information about members of the school community, even if the content is not shared publicly.
- Do not access or share material that infringes copyright, and do not claim the work of others as your own.
- Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities.
- Staff should not use their personal email, or social media accounts to contact students or parents, and students and parents should not attempt to discover or reach the personal email addresses or social media accounts of staff.

Using the school's IT systems

Whenever you use the school's IT systems you should follow these principles:

- Only access school IT systems using your username and password. Do not share your username or password with anyone else.
- Do not attempt to circumvent the content filters or other security measures installed on the school's IT systems, and do not try to access parts of the system that you do not have permission to access.
- Do not attempt to install software on, or otherwise alter, school IT systems.

- Do not use the school's IT systems in a way that breaches the principles of online behaviour set out above.

Remember that the school monitors the use of the school's IT systems and that the school can view content accessed or sent via its systems.

Compliance with related school policies

You will ensure that you comply with the school's E-Safety Policy, social media Policy, Safeguarding Policies and Anti-Bullying Policy.

Breaches of this policy

A deliberate breach of this policy will be dealt with as a disciplinary matter using the school's usual procedures. Also, a deliberate breach may result in the school restricting your access to school IT systems.

If you become aware of a breach of this policy or the E-Safety Policy, or you are concerned that a member of the school community is being harassed or harmed online, you should report it to the school's DSL. Reports will be treated with confidence.

Complaints relating to all aspects of E-Safety

As with all issues of safety, if a member of staff, a student or a parent/carer has a complaint or concern relating to

E-Safety prompt action will be taken to deal with it. Please see the Complaints Policy for further information.