LORDSWOOD SCHOOL

Online Safety Policy

Date: March 2026

Review Due: March 2027

Reviewed Annually

Introduction

Lordswood School's lead professional for Online Safety is the Head.

This policy has been written for Lordswood School, in line with local and national guidance.

This policy should be read in conjunction with the Safeguarding Policy (Child Protection), the Anti-bullying Policy and the PSHE & RSE Policy.

Background

At Lordswood School we understand the benefits and the risks associated with using the internet. This policy sets out clear procedures to ensure our pupils are safe and that they can learn how to use the Internet and ever-changing technologies in a safe and discerning way.

Adults, as well as young people, can find themselves vulnerable to malicious use of the Internet both in their personal and professional lives. This policy highlights the importance of training and guidance in good practice in safer use of the Internet for staff. The policy also recognises that there are other safety issues associated with using technologies, such as over-exposure to LCD screens, privacy etc.

The Internet and associated technology is a rapidly evolving environment where new opportunities and risks appear daily. Pupils learn to manage existing risks and understand the dynamic nature of technologies, so that they are able deal confidently with challenges in the future, whatever they might be.

1. Teaching and learning

As we move towards a more digital curriculum, we will actively promote the use of 'real-world' technologies to enhance and support learning.

1.1 Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school 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.

1.2 Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught the differences between acceptable and unacceptable Internet use.
- The school is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

1.3 Good Practice

- Teachers will update and check websites before accessing with the children to ensure that the content is appropriate. The curriculum is planned in context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; e.g. safe search kids or kiddle

- The school makes clear to all users what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and the curriculum plans.
- A record is kept of any Cyberbullying or inappropriate online behaviour in-line with the school behaviour management system. Parents/carers are informed of significant or repeated inappropriate behaviours
- The school ensures that all staff have appropriate training in Online Safety practice.
- The school provides advice and information on reporting offensive materials, abuse/ bullying etc and makes this available for pupils, staff and parents.
- Online Safety advice for pupils, staff and parents is provided.
- The school ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright / intellectual property rights.
- The school ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying online; online gaming / gambling.
- The school makes training about online safety available to staff and parents using The National College.
- The school gives advice, guidance and training for parents, including information leaflets; practical sessions and in the school newsletter.

1.4 Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law.
- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Lordswood has a clear, progressive Online Safety education programme throughout all Key Stages, built on local and national guidance. Pupils are taught a range of skills and behaviours appropriate to their age and experience, such as:

- to STOP and THINK before they CLICK
- to discriminate between fact, fiction and opinion;
- to develop a range of strategies to validate and verify information before accepting its accuracy;
- to skim and scan information;
- to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
- to know how to narrow down or refine a search;
- to understand how search engines work and to understand that this affects the results they see at the top of the listings;
- to understand 'Netiquette' behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
- to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
- to understand why online 'friends' may not be who they say they are and to understand why they should be careful in online environments;
- to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
- to understand why they must not post pictures or videos of others without their permission;
- to know not to download any files – such as music files - without permission;
- to have strategies for dealing with receipt of inappropriate materials;

- to understand online purchasing e.g. apps and within app purchases;
- to understand why and how some people will 'groom' others with inappropriate or illegal motives.

2. Managing Internet Access

2.1 Information system security

- School ICT systems capacity and security are reviewed regularly.
- Virus protection is updated regularly.

2.2 E-mail

- Pupils may only use approved school e-mail accounts on the school system.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

2.3 Published content and the school web site

- The contact details on the Web site are the school address, e-mail and telephone number. Staff, pupils' or governors' personal information will not be published.
- The Head will take overall editorial responsibility and ensure that content is accurate and appropriate.

2.4 Publishing pupil's images and work

- Photographs that include pupils will not refer to the pupil by full name. Digital images /video of pupils stored in a teacher's documents or shared images folder on the network are deleted at the end of the year – unless specifically required for a key school publication or assessment information.
- Images of children and staff are not to be taken on or away from school premises by parents or visitors, unless prior permission is sought and given by the school or at scheduled school events such as assemblies or festivals.
- Pupils are not identified by their full name in online photographic materials in the credits of any published school produced video materials / DVDs.
- Parental agreement is obtained, through Arbor on admission, before pupil's images are published on the school's website, social media accounts or other publications e.g. local newspapers. It is the responsibility of the parent/guardian to inform the school if this changes.
- Staff should ensure that pictures are removed from mobile phones / personal equipment before they leave the school premises.
- Pupils are taught about how images can be manipulated in their Online Safety education programme and also taught to consider how to publish for a wide range of audiences, which might include governors, parents or younger children.

2.5 Social networking and personal publishing (further details available in our Social Networking Policy)

- The school blocks/filters access to social networking sites or newsgroups unless there is a specific, approved educational purpose.
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Newsgroups will be blocked unless a specific use is approved.

- Pupils are advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents are advised that the use of some social network spaces, for example Facebook, Twitter, Instagram, X, WhatsApp outside school is inappropriate for primary aged pupils and that some of these sites have minimum age requirements.
- Pupils are taught that they should not post images or videos of others without their permission. They are taught about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. They are taught the need to keep their data secure and what to do if they are subject to bullying or abuse.

2.6 Managing filtering

- The school will work with relevant providers to ensure systems which protect pupils are regularly reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to SLT or Computing Lead. Concerns are escalated to the Technical service provider as necessary.
- The school will immediately refer any material we suspect is illegal to the appropriate authorities e.g Police, or the local authority.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

2.7 Managing emerging technologies

- Emerging technologies will be examined for educational benefit and an assessment will be carried out before use in school is allowed.
- Mobile phones will not be used for personal use during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

2.8 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and GDPR 2018.

3. Policy Decisions

3.1 Authorising Internet access

- The school reserves the right to withdraw Internet access from a pupil or member of staff in the event of misuse or infringement of policy.

3.2 Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor GST can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit computing provision to establish whether the Online Safety Policy is adequate and that its implementation is effective.

3.3 Handling Online 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 Head.
- Complaints of a child protection nature must be dealt with in accordance with school's child protection procedures.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

4. Communications Policy

4.1 Introducing the Online Safety policy to pupils

- Online Safety rules are discussed with the pupils on a regular basis.
- Pupils are informed that network and Internet use will be monitored.
- Pupils are not allowed to use mobile phones on the school site and should only be brought to school where a year 5 or 6 child walks to/from school without an adult.

4.2 Staff and the Online Safety Policy

- The Online Safety Policy is available to all staff and is included in child protection training sessions.
- Discretion and professional conduct are essential.

4.3 Enlisting parents' support

Parents/Carers' attention will be drawn to the school's Online Safety Policy in a variety of ways including: newsletters, open evening events and on the school web site. Courses will also be made available via The National College.

A range of resources and activities are available through:

- CEOP – Child Exploitation and Online Protection
- National Online Safety (via The National College)
- https://www.nspcc.org.uk/keeping-children-safe/online-safety/
- http://www.thinkuknow.co.uk
- https://www.internetmatters.org