Lode Heath School

Name of Policy	**Online Safety Policy**
Lead	Interim Gareth Davies, Assistant Headteacher
Governor Committee	BSII
Review Frequency	Annually
Next Review	Spring 2026
Version No.	2
Reviewed	January 2025

Policy Statement:

New technologies have become integral to the lives of young people in today's society, both within schools and in their lives outside school. Students need to develop high level computer skills, not only to maximise their potential use as a learning tool, but also to prepare themselves as lifelong learners and for future employment.

The purpose of this Online Safety Policy is to ensure that Lode Heath School meets its statutory obligations and that students are safe and protected from potential harm, both within and outside school. The policy will also form part of the school's protection from legal challenge, relating to the use of technology for teaching and learning.

Aims:

The requirement to ensure that students are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in Lode Heath School are bound.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote student achievement. The school will continue to investigate the appropriate use of artificial intelligence (AI) tools. However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content;
- Unauthorised access to/loss of/sharing of personal information;
- The risk of being subject to grooming by those with whom they make contact on the internet;
- The sharing/distribution of personal images without an individual's consent or knowledge;
- Inappropriate communication/contact with others, including strangers;
- Cyber bullying;
- Access to unsuitable video/internet games;
- An inability to evaluate the quality, accuracy and relevance of information on the internet;
- Plagiarism and copyright infringement, including the use of AI tools with assignments;
- Illegal downloading of music or video files;
- The potential for excessive use which may impact on the social and emotional development and learning of the student.

Many of these risks reflect situations in the off-line world and it is important that this Online Safety

Policy is used in conjunction with other school policies including the overarching Safeguarding Statement, Child Protection, Data Protection and Whole School Behaviour Policies as well as Acceptable User Guides for both staff and students.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

Legal Framework:

This policy applies to all members of the Lode Heath School community (including staff, students, volunteers, parents/carers, visitors, community users) who have access to and are users of school computer systems, both in and out of school.

The Education and Inspections Act 2006 empowers the headteacher, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber bullying, or other online safety related incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and the behaviour policy which includes anti-bullying and will, where known, inform parents/carers of incidents of inappropriate online behaviour that take place out of school.

Roles/ responsibilities:

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors BSII Committee receiving regular information about online safety incidents and monitoring reports.

Headteacher and Senior Leaders

- The Headteacher is responsible for ensuring the safety (including online safety) of members of the school

- The Headteacher and Senior Leaders are responsible for ensuring that all relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant

- The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff (see flow chart on dealing with online safety incidents – Appendix A, and relevant disciplinary procedures). The procedures for dealing with allegations against staff can be found within the school Child Protection Policy.

Network Manager/Technical staff

The Network Manager and Technical support staff are responsible for ensuring:

- that the school's IT infrastructure is secure and is not open to misuse or malicious attack;
- that the school meets the online safety technical requirements outlined in the Acceptable Use Policy that users may only access the school's networks through a properly enforced password protection policy
- the school's filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person;
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant;

- that the use of the network/Virtual Learning Environment (Microsoft Teams)/remote access/email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher or line manager for investigation/action/sanction;
- that monitoring of software and systems are implemented and updated

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up-to-date awareness of online safety matters and of the current school Online Safety Policy and practices;
- they have read, understood and signed the school Staff Acceptable Use Policy
- they report any suspected misuse or problem to either a Head of Year, member of SLT or the Network Manager and his team as appropriate
- digital communications with students/students (email/Microsoft Teams/ video or voice) should be on a professional level and only carried out using official school systems;
- online safety issues are embedded in all aspects of the curriculum and other school activities;
- students/students understand and follow the school online safety and acceptable use policy
- students/students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- they monitor IT activity in lessons, extra-curricular and extended school activities;
- they are aware of online safety issues related to the use of mobile phones, cameras, tablets, smart watches and other hand held devices and that they monitor their use and implement current school policies with regard to these devices;
- in lessons, where internet use is pre-planned, students/students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Designated Safeguarding Lead (DSL)

Will be trained in online safety issues and be aware of the potential for serious child protection issues to arise from: • sharing of personal data;

- access to illegal/inappropriate materials;
- inappropriate on-line contact with adults/strangers;
- potential or actual incidents of grooming;
- cyberbullying;
- potential for peer on peer abuse

Students

- are responsible for using the school computer systems in accordance with the Student Acceptable Use Policy (AUP), which they and/or their parents/carers will be expected to sign before being given access to school systems;
- need to have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- will be expected to know and understand school policies on the use of mobile phones, smart watches, digital cameras, tablets and other hand held devices. They should also know and understand school policies on the taking/use of images and on cyber bullying;
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of computers than their children. The school will therefore take every opportunity to help parents understand these issues through newsletters, the school website and information about national/local online safety campaigns/literature.

Parents and carers will be responsible for:

- endorsing (by signature) the Student Acceptable Use Policy (AUP**)**
- accessing the school website in accordance with the relevant school Acceptable Use Policy.
- ensuring that they themselves do not use the internet/social network sites/other forms of technical communication in an inappropriate or defamatory way

Community Users

Community Users who access school systems as part of the Extended School provision will be expected to sign an AUP before being provided with access to school systems

Managing Filtering

Levels of Internet access and supervision will vary according to the student's age and experience. Access profiles must be appropriate for all members of the school community. Older secondary students, as part of a supervised project, might need to access specific adult materials; for instance a course text or set novel might include references to sexuality. Teachers might need to research areas including drugs, medical conditions, bullying, racism or harassment. In such cases, legitimate use should be recognised and restrictions removed temporarily.

Filtering is not 100% effective. There are ways to bypass filters (such as using proxy websites, using a device not connected to the network e.g. smart phone, smart watches). It is therefore important that students are supervised when using internet access and that Acceptable Use Policies are in place. Any material that the school believes is illegal must be reported to appropriate agencies.

- The school's internet access will include filtering appropriate to the age and maturity of students.
- The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all students) will be aware of this procedure.
- If staff or students discover unsuitable sites, the URL will be reported to the Network Manager, who will action the concern as appropriate.
- The School filtering system will block all sites on the Internet Watch Foundation (IWF) list
- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team.
- The School Senior Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective.
- Any material that the school believes is illegal will be reported to appropriate agencies
- The school's access strategy will be designed by educators to suit the age and curriculum requirements of the students, with advice from network managers.