Lady Margaret School

Online Safety Policy

Reviewed: February 2020
Next Review: February 2023

1 Introduction and Overview

Our aim is that all our students will use social media safely, act with integrity and honesty online as they would in real life, and report anything which is dangerous or causes them concern.

1.1 Rationale - the purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Lady Margaret School with respect to the use of ICT-based technologies.
- Safeguard and protect the students and staff of Lady Margaret School
- Assist school staff working with students to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

1.2 The main areas of risk for our school community can be summarised as follows:

1.2.1 Content

Exposure to inappropriate content, including but not limited to:

- online pornography
- ignoring age ratings in games (exposure to violence associated with often racist language),
- substance abuse
- Political or religious extremism
- Lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- Hate sites including those expressing racist views
- Content validation: how to check authenticity and accuracy of online content

1.2.2 Contact

- Grooming
- Cyber-bullying in all forms
- Identity theft including hacking social media profiles and sharing passwords

1.2.3 Conduct

- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online (Internet or gaming))
- Sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- Copyright (little care or consideration for intellectual property and ownership – such as music and film)

1.3 Scope

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

The Education and Inspections Act 2006 empowers Headteachers / Principals to such extent as is reasonable, to regulate the behaviour of students when they are off the Lady Margaret 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 incidents covered by this policy, which may take place outside of the school, but are linked to membership of the school.

Lady Margaret School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school. In addition, the school will actively cooperate with the police and other agencies to identify and sanction offenders.

Role	Key Responsibilities
Headteacher	• To take overall responsibility for onlinesafety provision • To take overall responsibility for data and data security • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements e.g. LGfL (London Grid for Learning) • To be responsible for ensuring that staff receive suitable training to carry out their online safety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious online safety incident. • To ensure that there is a system in place to monitor and support staff who carry out internal online safety procedures (e.g. network manager)
SLT and HOYs Director of Sixth Form	• To take day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents • To promote an awareness and commitment to online safeguarding throughout the school community • To ensure that online safety education is embedded across the curriculum • To liaise with school ICT technical staff • To communicate regularly with SLT and the designated online safety Governor /

Role	Key Responsibilities
	committee to discuss current issues, review incident logs and filtering / change control logs • To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident • To log all online safety incidents • To facilitate training and advice for all staff • To liaise with the Local Authority and relevant agencies • Are regularly updated in online safety issues and legislation, 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 • cyber-bullying and use of social media
Governors / Online safety Governor	• To ensure that the school follows all current online safety advice to keep the students and staff safe • To approve the Online Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors / Governors Sub Committee receiving regular information about online safety incidents and monitoring reports. Nicky Thomson, a member of the Governing Body has taken on the role of Online Safety Governor • To support the school in encouraging parents and the wider community to become engaged in online safety activities • The role of the Online Safety Governor will include: • regular review with the Online Safety Co-ordinator (including online safety incident logs, filtering / change control logs)
Police School Liaison Officer	• PSHE support • Online Safety • Fraud • Sexting • Help with all online queries • Handling complaints

Role	Key Responsibilities
IT Dept	• To report any online safety related issues which arise to the SLT. • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date • To ensure the security of the school ICT system • To ensure that access controls exist to protect personal and sensitive information held on school-owned devices • To ensure the school's policy on web filtering is applied and updated on a regular basis • To ensure LGfL is informed of issues relating to the filtering applied by the Grid • To keep up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant • To ensure that the use of the network remote access and email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator for investigation and, if necessary, sanction. • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To ensure that all data held on students on the school machines have appropriate access controls in place. • To ensure all LGfL services are managed on behalf of the school including maintaining the LGfL USO database of access accounts.
Teachers	• To embed online safety issues in all aspects of the curriculum and other school activities • To supervise and guide students carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) • To ensure that students are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.
All staff	• To read, understand and help promote the school's online safety policies and guidance • To read, understand and adhere to the school Use of ICT Network and Equipment Policy • To understand and adhere to the school policy on passwords. • To be aware of online safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current school policies with regard to these devices • To report any suspected misuse or problem to the online safety coordinator • To maintain an awareness of current online safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with students should be on a professional level and only through school-based systems including school email.

Role	Key Responsibilities
Students	• Read, understand, sign and adhere to the Pupil Acceptable Use Policy for ICT • have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • to understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology. • To know and understand school policy on the use of mobile phones, digital cameras and hand-held devices. • To know and understand school policy on the taking / use of images and on cyber-bullying. • To 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 • To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home • To help the school in the creation/ review of online safety policies • To understand that their use of the school network and school email is monitored. • In addition, some students have been asked to participate in a peer mentoring scheme.
Parents/carers	• To support the school in promoting online safety by signing and endorsing Pupil Acceptable Use Policy for ICT • To consult with the school if they have any concerns about their daughters' use of technology • To not upload to social media sites or other public websites any photographs or videos of LMS students unless the image is solely of their own child(ren)

1.4 Communication:

The policy will be communicated to staff/students/community in the following ways:

- Policy to be posted on the school website
- Policy to be part of school induction pack for new staff
- Pupil Acceptable Use Policy for ICT discussed with students and signed by students and parents at the start of each year.

1.5 Handling complaints

- The school will take all reasonable precautions to ensure online safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

- Staff and students are given information about infringements in use and possible sanctions. Sanctions available include:

  - interview/counselling by Form Tutor/Heads of Year/SLT/Headteacher;

  - informing parents or carers;
  - removal of Internet or computer access for a period,
  - referral to LA / Police.

- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LA child protection procedures.

1.6 Review and Monitoring

The online safety policy is referenced from within other school policies: Use of ICT Network and Equipment policy, Child Protection policy, Data Protection policy, Anti-Bullying policy and Behaviour policy.

- The online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school
- The online safety policy has been written by the school Headteacher and is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school e-safeguarding policy will be discussed in detail with all members of teaching staff.

2 Procedures

2.1 Education and Curriculum

2.1.1 Student online safety curriculum

This school:

- Has a clear, progressive online safety education programme as part of the PSHE curriculum. It is built on LGfL and national guidance. This covers a range of skills and behaviours appropriate to their age and experience, including:
  - to STOP and THINK before they CLICK
  - to develop a range of strategies to evaluate and verify information before accepting its accuracy;
  - 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 acceptable 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 on-line ‘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;
    - [for older students] to understand why and how some people will ‘groom’ young people for sexual reasons;
    - To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
    - To be aware of the role and function of extremist recruitment sites.
    - To know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.

- Plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind students about their responsibilities through a Pupil Acceptable Use Policy for ICT which every student will sign and keep in their daybooks.
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensures that when copying materials from the web, staff and students understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights;
- Ensures that staff and students understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling;

2.1.2 Staff and governor training

This school:

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to adequately secure any school data on devices they are using
- Makes regular training available to staff on online safety issues and the school’s online safety education program.
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the Safeguarding Policy and the school’s Online Safety Policy.

2.1.3 Parent awareness and training

This school

- Runs a rolling programme of advice, guidance and training for parents, including:
    - Yearly Pupil Acceptable Use Policy for ICT, to ensure that principles of e-safe behaviour are made clear
    - Yearly mailings sent home with suggestions for safe Internet use at home and provision of information about national support sites for parents. These mailings are also made available on the school website

2.2 Expected Conduct and Incident management

2.2.1 Expected conduct

In this school, all users:

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy for ICT which students will be expected to sign before being given access to school systems and the Use of ICT Network and Equipment policy which covers staff use of ICT.
- need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- 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
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand-held devices. They should also know and understand school policies on cyber- bullying

Staff

- are responsible for reading the school's online safety policy and Use of ICT Network and Equipment policy and using the school ICT systems accordingly.

Students

- should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

Parents/Carers

- should know and understand what the 'rules of appropriate use' are and what sanctions result from misuse

2.2.2 Incident Management

In this school:

- there is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive.
- all members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively.
- support is actively sought from other agencies as needed (e.g. the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with online safety issues. The school will actively cooperate with the police and other agencies to identify and sanction offenders.

- monitoring and reporting of e safety incidents takes place and contribute to developments in policy and practice in online safety within the school. The records are reviewed/audited and reported to the school’s senior leaders and Governors
- parents / carers are specifically informed of online safety incidents involving young people for whom they are responsible.
- Students are able to speak to specially trained peer mentors to discuss online safety issues.