Lady Manners School

Online Safety Policy

Policy No:	050
Reviewed by:	DR
Approved by:	Governors' Curriculum and Students Committee
Minute No:	CS24/25
Review Cycle:	Annual
Last Reviewed:	28 January 2025
Next Review Date:	January 2026

Through our shared school values, we aim for all students to thrive, feel included and aspire to grow as individuals who contribute to society with empathy, integrity and positivity.

This document will be reviewed annually by the Governors' Curriculum and Students Committee and sooner when significant changes are made to the law.

Guidance from the Department for Education about school policies can be found here: https://www.gov.uk/government/publications/statutory-policies-for-schools-and-academy-trusts/statutory-policies-for-schools-and-academy-trusts

Contents

EQUALITIES STATEMENT OF INTENT

Lady Manners School welcomes a diverse population of both students and staff. In order to consolidate and build upon this diversity, equality of opportunity and the absence of unfair discrimination is at the core of all the school's activities. The school will not unfairly discriminate in the recruitment or general treatment of staff or students.

The school is committed to promoting and developing equality of opportunity in all its functions and will seek to do this by:

- communicating its commitment to equality and diversity to all members of the school community;
- maintaining systems for implementation, monitoring, evaluation and review;
- treating acts of discrimination and other contraventions of this policy as a disciplinary offence.

The Governing Board has responsibility for ensuring that the school operates within the legal framework for equality and for implementing the policy throughout the school. In addition, each member of the school community is responsible for preventing unfair discrimination or harassment or victimisation which it is within their control to prevent; and challenging or reporting such inappropriate behaviour if it occurs.

1. INTRODUCTION

1.1 At Lady Manners School, we understand that online technologies can be an essential resource for supporting teaching and learning. They open up opportunities for students and play an important role in their everyday lives.

1.2 The purpose of this online safety policy is to:

- Safeguard and protect all members of Lady Manners School community online.

- Identify approaches to educate and raise awareness of online safety throughout the community.

- Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.

- Identify clear procedures to use when responding to online safety concerns.

1.3 This school identifies that the issues classified within online safety are considerable, but can be broadly categorised into four categories of risk:

- **Content:** being exposed to illegal, inappropriate or harmful material, such as pornography, fake news, racism, misogyny, self-harm, suicide, religious intolerance, radicalisation and extremism

- **Contact:** being subjected to harmful online interaction with other users, such as 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:** personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual 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

2. LEGISLATION AND GUIDANCE

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate

images or files on students' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. LINKS WITH OTHER POLICIES AND PRACTICES

This policy links with several other policies, practices and action plans including:

Anti-bullying Policy
Code of Conduct
Behaviour for Learning Policy
Safeguarding and Child Protection Policy
Guidance for Safer Working Practice
Relationships and Sex Education (RSE) Policy
Remote Learning Policy

4. ROLES AND RESPONSIBILITIES

- The Governing Board has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

- The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

- The Designated Safeguarding Lead (DSL) has lead responsibility for online safety.

- Lady Manners School recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

4.1 The Designated Safeguarding Lead (DSL) will:

- Ensure there are appropriate and up-to-date policies regarding online safety; including a staff code of conduct *and* acceptable use policy, which covers acceptable use of technology.
- Ensure that staff understand this policy and that it is being implemented consistently throughout the school
- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Work alongside deputy DSLs to ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations
- Take the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Work alongside the network manager to ensure that the appropriate systems and processes in relation to online safety are in place

- Ensure that online safety is embedded within the curriculum, which enables all students to develop an age-appropriate understanding of online safety.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant knowledge and up to date required to keep students safe online and recognise the additional risks that students with SEN and disabilities (SEND) face online.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Address any online safety issues or incidents in line with the school's child protection policy
- Maintain records of online safety concerns, as well as actions taken, as part of the school's safeguarding recording systems.
- Review this policy annually and ensure the procedures and implementation are updated and reviewed regularly

4.2 It is the responsibility of all members of staff to:

- Read and adhere to the IT Policy.
- Take responsibility for the security of setting systems and the data they use or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the school's safeguarding policies and procedures.
- Know that the DSL is responsible for the filtering and monitoring systems and processes, and be aware of how to report any incidents of those systems or processes failing by notifying the DSL and the network manager
- Working with the DSL to ensure that any online safety incidents are logged on cpoms) and dealt with appropriately
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'
- Take personal responsibility for professional development in this area.

4.3 It is the responsibility of the network manager to:

- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Ensuring that the school's IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Implement appropriate security measures as directed by the DSL and leadership team such as enforcing industry standard password policies and encrypting sensitive data to ensure that the settings IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Put in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Ensure appropriate access and technical support is given to the DSL (and/or deputy) to our filtering and monitoring systems, to enable them to take appropriate safeguarding action if/when required.

4.4 It is the responsibility of students (at a level that is appropriate to their individual age and ability) to:

- Engage in age appropriate online safety education opportunities.
- Read and adhere to the acceptable use policies.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

4.5 It is the responsibility of parents and carers to:

- Read the acceptable use policies and encourage their children to adhere to them.
- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from school, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Use our systems, such as learning platforms, and other network resources, safely and appropriately.

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet
- Parent resource sheet – Childnet

5. EDUCATION AND ENGAGEMENT APPROACHES

5.1 Education and engagement with students

- An online safety programme is established and taught across the curriculum, ensuring that students are aware of the safe use of technology and Artificial Intelligence both inside and outside of the school. Methods of delivery will include Computing, Personal Development lessons, assemblies, tutorial and pastoral activities.

  In **KS3**, students will be taught to:

  - Understand a range of ways to use technology and Artificial Intelligence safely, respectfully, responsibly and securely, including protecting their online identity and privacy
  - Recognise inappropriate content, contact and conduct, and know how to report concerns

  Students in **KS4** will be taught:

  - To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
  - How to report a range of concerns

  By the **end of secondary school**, students will know:

  - Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
  - About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
  - Not to provide material to others and Artificial Intelligence that they would not want shared further and not to share personal material that is sent to them
  - What to do and where to get support to report material or manage issues online
  - The impact of viewing harmful content
  - That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others, and negatively affect how they behave towards sexual partners
  - That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail

- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

5.2 Vulnerable Students

- Lady Manners School recognises that some students are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.
- Lady Manners School will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable students.

5.3 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim. The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes Personal Development and Computing and other subjects where appropriate.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

5.4 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or students, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Assess how urgent the search is, and consider the risk to other students and staff. If the search is not urgent, they will seek advice from the headteacher / DSL
- Explain to the student why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the student's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / headteacher / other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The student and/or the parent/carer refuses to delete the material themselves
- If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of students will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

5.5 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, students and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Lady Manners School recognises that AI has many uses to help students learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Lady Manners School will treat any use of AI to bully students in line with our anti-bullying/behaviour policy.

6 ACCEPTABLE USE OF THE INTERNET IN SCHOOL

All students, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

6.1 Training and engagement with staff

We will:

- Provide and discuss the online safety procedures with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff, including governors where relevant to their role on a regular basis.
- Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns
- Make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- Make staff aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the students.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting students, colleagues or other members of the community.

7. USEFUL LINKS FOR EDUCATIONAL SETTINGS

Derbyshire Police:

- In an emergency (a life is in danger or a crime in progress) dial 999.

For other non-urgent enquiries contact Derbyshire Police via 101

LADO

- By referral into Professional.Allegations@derbyshire.gov.uk
- Form found here

http://derbyshirescbs.proceduresonline.com/docs_library.html

Call Derbyshire (Starting Point)

- Immediate risk of harm phone 01629 533190
- For all other referrals complete an online form

https://www.derbyshire.gov.uk/social-health/children-and-families/support-for-families/starting-point-referral-form/starting-point-request-for-support-form.aspx

- For professional advice phone 10629 535353

National Links and Resources for Educational Settings

- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org

- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
  - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
  - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- 360 Safe Self-Review tool for schools: www.360safe.org.uk

National Links and Resources for Parents/Carers

- Action Fraud: www.actionfraud.police.uk
- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
  - ChildLine: www.childline.org.uk
  - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk