LADYBROOK PRIMARY SCHOOL

E SAFETY POLICY

including Acceptable Use

Date Policy Adopted by Governing Body			
Autumn 2021 (Following review of original policy in July 2021)			
REVIEW SCHEDULE			
Date of Next Review	Date reviewed by governing body	Change previous document Y/N	Date circulated (If changes are made)
Autumn 2021	19.10.21	Y	
Autumn 2023	31.1.23	N	
Autumn 2025	03.10.25	Y	10.10.25
Autumn 2027			

This policy should be read alongside other school policies, particularly:

Safeguarding Policy
Anti-Bullying Policy
Relationships and Behaviour Policy
Staff Code of Conduct (See Staff Handbook)
Confidential Reporting Policy (Whistleblowing)
Complaints Procedure
Respect policy

This E safety (Online) policy, incorporating Acceptable Use of digital tools, has been reviewed by

Computing Lead / E Safety Leader - Rebecca Foley
Head teacher – Caroline Woosnam

This policy has been agreed by the school senior leadership team and the governing body. The online safety policy will be reviewed annually, or more regularly in the light of significant developments in the use of technologies, new threats to online safety or incidents that have taken place.

The computing lead will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)/filtering
- Internal monitoring data for network activity
- Surveys/questionnaires of staff/parents/carers
- Pupil voice reviews
- Annual parent Questionnaire

Introduction

The purpose of Internet access in schools is to raise educational standards, to support the professional work of staff and to enhance the school's management information and business administration systems. Access to the Internet and use of technology such as cameras are necessary tools for staff and an entitlement for pupils who show a responsible and mature approach. It should be noted that the use of a computer system without permission or for a purpose not agreed by the school could constitute a criminal offence under the Computer Misuse Act 1990. It is our aim to have a clear policy on the acceptable use of the internet, mobile phones and cameras that is understood and adhered to by all parties concerned without exception.

The computer system is owned by the school and may be used by pupils to further their education and by staff to enhance their professional activities including teaching, research, administration and management. The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.

E Safety Policy

This policy applies to all members of the Ladybrook community (including staff, Ladybrook pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school digital technology systems, both in and out of the school.

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

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

Governors

Governors are responsible for the approval of the E-safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about any online safety incidents and monitoring reports.

Headteacher and SLT

The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the computing lead.

The Headteacher and (at least) another member of the Senior Leadership Team

1. 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 confidential Reporting Policy –disclosure Form)
2. Are responsible for ensuring that the E Safety / Computing Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
3. Will receive regular monitoring reports from the Online Safety Lead.

Online Safety Lead

1. Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents
2. Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
3. Provides training and advice for staff
4. Liaises with school technician and business manager

5. Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments. (See Appendix 1)
6. Reports to Senior Leadership Team if an E-Safety issue has occurred.
7. Monitors planning to ensure safety is being taught across the school in all year groups.
8. Ensures all Ks2 children are aware of the Pupil E safety Acceptable Use Agreement and staff encourage pupils to follow them when using technology.
9. Ensures that staff are fully aware of their professional responsibilities when using the internet.

Network Manager/Technical staff (HG IT)

Those with technical responsibilities are responsible for ensuring that:

1. The school's technical infrastructure is secure and is not open to misuse or malicious attack
2. The school meets required online safety technical requirements and Stockport's online safety guidance.
3. Users may only access the networks and devices through a properly enforced password protection policy
4. A filtering system is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
5. They keep up to date with online safety technical information to effectively carry out their online safety role and to inform and update others as relevant
6. The use of the networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher and Senior Leaders / Online Safety Lead
7. Monitoring software/systems are implemented and updated as agreed in school policies

Teaching and Support Staff

Are responsible for ensuring that:

1. They have an up-to-date awareness of online safety matters and of the current school online safety policy and practices
2. They have read, understood and signed the Staff Code of Conduct (Appendix 3) for Computing and ICT
3. They report any suspected misuse or problem to the Headteacher/ Senior Leader/Online Safety Lead for investigation.
4. All digital communications with Ladybrook pupils/parents/carers should be on a professional level and only carried out using official school systems
5. Online safety issues are embedded in all aspects of the curriculum and other activities
6. They monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
7. In lessons where internet use is pre-planned Ladybrook pupils 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 – (see Appendix 4 for a list of child friendly search engines)

Designated Safeguarding Lead

Should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding 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
- Online-bullying
- An understanding of disinformation and misinformation

Ladybrook pupils

Are responsible for ensuring that they:

1. Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
2. Are responsible for using the school digital technology systems in accordance with the **Pupil E safety Acceptable Use Agreement**
3. Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
4. Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online-bullying.
5. Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's/academy'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. The school will take every opportunity to help parents understand these issues through newsletters, website – E Safety section and information about national/local online safety campaigns/literature. Parents and carers will be encouraged to support the school in promoting good online safety practice through the E-Safety Acceptable Use Agreement (Appendix 2) and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website/Learning Platform and on-line student/pupil records
- When using Google Classroom for remote learning

Education – Ladybrook pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils at Ladybrook to take a responsible approach. The education of Ladybrook pupils in online safety/digital literacy is therefore an essential part of our safety provision.

To plan our online safety curriculum Ladybrook staff use the following resources:

https://www.1decision.co.uk/
https://beinternetawesome.withgoogle.com/en_uk/
https://www.discoveryeducation.co.uk/resources/primary/espresso/
https://www.childnet.com/resources/smartie-the-penguin
https://www.thinkuknow.co.uk/

Online safety is a focus in all areas of the curriculum and Ladybrook staff reinforce online safety messages across the curriculum. The online safety curriculum is broad, relevant and provide progression, with opportunities for creative activities and provides in the following ways:

- A planned online safety curriculum is provided as part of Computing/PHSE/other lessons and is regularly revisited
- Key online safety messages are reinforced throughout the year when using technology
- Ladybrook pupils are taught in all lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of information.
- Ladybrook pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Ladybrook pupils are supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Ladybrook pupils are helped to understand the need for the **Pupil E safety Acceptable Use Agreement** and encouraged to adopt safe and responsible use both within and outside school.
- Staff act as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where internet use is pre-planned Ladybrook pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where Ladybrook pupils are allowed to freely search the internet, staff are vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g., racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents/carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- The Online safety section of the school website https://www.ladybrook.stockport.sch.uk/online-safety/
- Organised parent meetings with safety expert
- High profile events/campaigns e.g., Safer Internet Day / Anti Bullying Week
- Reference to the relevant web sites/publications e.g., swgfl.org.uk, www.saferinternet.org.uk/, http://www.childnet.com/parents-and-carers (See appendix for further links/resources)

Artificial Intelligence (AI) in Education

AI is becoming more common in schools and can be used to support learning and reduce teacher workload. It offers opportunities for personalised learning but also raises important issues around data privacy, fairness, and safe use.

At Ladybrook Primary, we will:
Use AI carefully to enhance teaching and learning.
Ensure staff receive support and training to use AI tools effectively.
Teach children to use AI responsibly as part of developing their digital skills.
Follow clear ethical guidelines to protect pupils' wellbeing and ensure fairness.
Our aim is to use AI in a way that is safe, responsible, and beneficial for all learners.

Use of AI in teaching and learning:

AI may be used to enhance teaching and learning.
AI tools will be used purposefully and only where there is a clear educational benefit.
Pupils will be taught about the benefits and risks of AI and how to use it responsibly.

Responsibilities for Staff
All staff are expected to use AI professionally and responsibly:

By protecting sensitive and personal data by not entering identifiable information into AI systems.
By following UK GDPR and all relevant data protection legislation.
By fact-checking and critically reviewing AI outputs before using or sharing them.
By reporting any incidents involving misuse, data breaches, or inappropriate AI outputs immediately.
By recognising that AI is to assist, not replace, human decision-making.

Training will be provided to staff to ensure confidence in using AI safely and effectively.

Responsibilities for Pupils
Pupils will:

Learn how AI works, what it can do and its risks and benefits.
Use AI responsibly and fairly, following the school's Acceptable Use Agreement.
Understand that AI can support their learning but must not replace their own ideas or creativity.
Be encouraged to question and think critically about AI-generated content.

Safeguarding, Data Protection & Ethics

The school will comply with all relevant legislation, including KCSiE and UK GDPR.
Sensitive or internal school information **must not** be entered into third-party AI tools.
The computing coordinator will monitor AI tools in use.
AI tools will not be used in a way that discriminates unfairly or misuses intellectual property.
Staff must ensure that pupils' work, photographs and personal information are protected and not used in any AI tools.

Managing Information Systems

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet or taken off site will be encrypted.
- All memory sticks used in school will be encrypted with a password.
- Work kept in Google Shared drives can only be accessed by staff who have been given permission.
- Unapproved software will not be allowed in pupils' work areas or attached to email.
- Files held on the school's network will be regularly checked and/or Google Drive
- The ICT team (i.e Computing leader/ technician and business manager) will review system capacity regularly.

Data Protection

Data that the school holds shall be

- Processed fairly and lawfully
- Processed for specific purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Held no longer than necessary
- Kept secure

Email and communication

The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and Ladybrook pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g., by remote access).

Users must immediately report to the nominated person – in accordance with the school policy, 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.

Any digital communication between staff and Ladybrook pupils or parents/carers (email, Twitter, Google Classroom) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.

Pupils may only use approved email accounts on the school system – each child has a Gmail account for accessing the Google Classroom. Pupils may only communicate with other members of the school network – their classmates.

Ladybrook pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

School Website

The contact details on the website are the school address, email and telephone number. Staff or pupils' personal information must not be published.
Each class teacher is responsible for updating their own class page half termly, ensuring any photos do not contain personal information.

The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.
Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Images of pupils should not be published without the parent/carer's permission. Images of pupils must be selected carefully. All staff should be aware of children in their class who do not have consent for the image to be published online. Pupils' full names will not be used anywhere on the website, particularly in association with photographs.

Social Media

Ladybrook Primary School has a duty of care to provide a safe learning environment for pupils and staff. The school could be held responsible, indirectly for acts of their employees in the course of their employment.

Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

Ladybrook Primary school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through ensuring that personal information is not published.

School staff should ensure that:

- No reference is made in social media to Ladybrook pupils, parents/carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official school social media accounts are established, there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under school disciplinary procedures

Mobile Phones in school - Children

Mobile phones are now a feature of modern society and an increasing number of our staff and pupils own one. The increasing sophistication of mobile phone technology presents several issues for schools:

- The high value of many phones
- The integration of cameras into phones leading to potential child protection and data protection issues
- The potential to use the phone e.g., for texting whilst on silent mode
- Children are not allowed mobile phones in school at any time.
- Mobile phones are not allowed in school at any time.
- On some occasions for safety reasons, parents need to have contact with a child e.g., walking home. Therefore, any children needing their phone for safety reasons must hand their phone into the school office on entering school. The phone must be switched off (not on silent mode)
- If a child breaches these rules the phone will be confiscated and given into the main office. It will be returned to the child after a discussion with parents.

Smart watches – Children

Smart watches have the facility to record still and video images. Some smart watches can be accessed from outside the building, for example, individuals outside of the building listening in to conversations and tracking children's actions. All of these capabilities form potential safeguarding issues. Smartwatches are therefore not permitted to be worn to school as staff are unable to monitor them closely enough to ensure they are being used appropriately. However, in line with our passion for helping children to tell the time, a standard analogue or digital wrist watch may be worn. If you are unsure whether your child's watch is appropriate, please speak to the headteacher.

Health devices that only have the ability to tell the time and track activity are permitted.

Staff mobile phones

Ladybrook Primary School allows staff to bring in personal mobile telephones and devices for their own use. Members of staff should use their personal devices with caution and as a last resort, if needing to contact a pupil or parent.

- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- It is the responsibility of all members of staff to be vigilant and report any concerns to the Headteacher.
- Concerns will be taken seriously, logged and investigated appropriately.
- Should inappropriate material be found then our Local Authority Designated Officer (LADO) will be contacted immediately. We will follow the guidance of the LADO as to the appropriate measures for the staff member's disciplinary action.
- Phones must not be used for any purpose during lesson time.
- Phones must be stored out of sight during lesson time and meeting time.

- Phones must always be switched off or on silent mode during class time and meeting time unless permission has been granted in advance by senior staff.

Smart watches – Staff

Ladybrook Primary School allows staff to wear Smart Watches with the following criteria:
Smart watches have the capability to record still and video images. This poses a safeguarding issue. Staff wearing a smart watch with these capability should disable these features during the work day.
Smart watches also have the ability to receive calls and messages. In-line with our mobile phone policy, watches should be silenced (including notifications) or set to 'work mode' during the teaching day. This will disable incoming calls and messages. Staff should not be checking messages on any device during teaching time unless permission has been granted in advance by senior staff for a specific reason.

Emergencies

If a child needs to contact his/her parents/guardians, they will be allowed to use a school phone under adult supervision.

If parents need to contact children urgently, they should phone the school office and a message will be relayed promptly.

Responsibility for mobile phones

School accepts no responsibility whatsoever for theft, loss, damage or health effects (potential or actual) relating to mobile phones. It is the responsibility of staff, parents and children to ensure mobile phones are properly insured.

Photographs

Photographs and videos taken for the purpose of recording a child or group of children participating in activities or celebrating their successes is an effective form of recording their achievements. However, it is essential that photographs are taken and stored appropriately to safeguard the children in our care.

- Designated school cameras/ iPad are to be used to take any photo within the setting or on outings.
- Images taken on a camera or iPad must be deemed suitable without putting the child/children in any compromising positions that could cause embarrassment or distress.
- All staff are responsible for the security of the cameras/ iPad.
- Images taken and stored on the camera must be downloaded as soon as possible.
- If the technology is available images should be downloaded on-site. Should these facilities not be available, these may be downloaded off-site and erased from the personal computer as soon as the images are no longer relevant to the teachers' work.
- Personal mobile phones should not be used as a camera by staff and/or parents.

E-safety complaints

Complaints of misuse will be dealt with under the school's Complaints procedure. Any complaint about staff misuse must be referred to the head teacher via the computing coordinator.

- All E-safety complaints and incidents will be recorded by the school, the safeguarding lead may also be informed depending on the nature of the incident. Any actions taken must also be recorded.
- Parents/carers will be informed of the complaint's procedure
- Parents/carers/pupils will work in partnership with staff to resolve issues.

- A log will be kept by the computing coordinator/safeguarding lead.
  (See appendix 2)

Cyberbullying

Cyberbullying (along with all forms of bullying) will not be tolerated in school. Full details can be found in the school's Anti-Bullying Policy.

- All incidents of cyber bullying reported to school will be recorded by the E safety lead/safeguarding officer.
- Pupils, staff, parents and carers will be advised to keep a record of the bullying as evidence.
- Parents/carers of children involved will be informed
- Pupils will be asked to remove any material deemed inappropriate or offensive.

Appendix 1: **Log of cyberbullying / E Safety incident**

Date/Time	Person/Persons reporting:
Description of the Incident/s:	
How Incident was dealt with:	
Follow up action:	

Appendix 2: Pupil / Parent / Carer E-safety Acceptable Use Agreement

All pupils at Ladybrook Primary School have access to computing facilities including access to the internet as an essential part of their learning, as required by the National Curriculum.
All pupils and their parents/carers are asked to sign to show that the ESafety rules at Ladybrook Primary have been understood and agreed.

Pupil:	Year group:

Pupil's Agreement

- I have read and understood the school e Safety Guidelines.
- I will always use computing technology – Chrome Books/iPad/laptops/computers/cameras etc in a responsible way.
- I will use the internet access for teacher directed tasks only and know what to do if something I see is not appropriate.
- I know that my network and internet access may be monitored

Signed:	Date:

Parent's Consent for Internet Access

- I have read and understood the E Safety guidelines for Ladybrook and give permission for my son / daughter to access the internet.
- I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials and will use the internet under teacher direction.

Parents/Carers should:

- Discuss eSafety issues with my child/children.
- Ensure my child access age-appropriate websites, social media and games.
- Ensure that where my child communicates online, they are respectful and responsible.
- Inform the school if there is an E Safety issue related to the school.
- Maintain their own responsible standards and communicate respectively about Ladybrook Primary school when communicating on social media and the internet.

Signed:	**Date:**

Appendix 3: Staff Code of Conduct for Computing and E Safety.

To ensure all members of staff at Ladybrook Primary School are aware of their professional responsibilities when using computing technology and the internet, they are required to sign this code of conduct for computing and eSafety.
All members of staff should consult the Ladybrook eSafety policy for further information, guidance and clarification.

- I understand that it is a criminal offence to use school computing and ICT systems for a purpose not permitted by its owner.
- I understand that school information systems may not be used for private purposes without specific permission from the Headteacher.
- I understand it is my responsibility to report any suspected misuse or problem with technology or internet access to the Headteacher/ Senior Leader/Online Safety Lead for investigation.
- I understand digital communications with Ladybrook pupils/parents/carers should be on a professional level and only carried out using official school systems.
- I understand online safety issues are embedded in all aspects of the curriculum and other activities. I am aware of online safety matters and of the current school online safety policy and practices and promote online safety with students in my care. I will help them develop a responsible attitude to system use and communications.
- I am responsible for monitoring the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies regarding these devices.
- I will report any incidents of concern regarding children's safety to the computing coordinator / designated Safeguarding lead or the Headteacher.
- I understand that any photographs taken of pupils should be respectful and taken on the school's equipment. Where the school's equipment is not available and personal equipment is used, images should be uploaded and deleted as soon as possible.
- I understand in lessons where internet use is pre-planned Ladybrook pupils 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 – (see appendix 5 for a list of child friendly search engines)

I have read, understand and accept the staff Code of Conduct for Computing and E-Safety.

Name:	Date:
Signed:	

Appendix 4: Ladybrook Safe Websites for Children

http://www.kidtopia.info/

https://teachthechildrenwell.com/

http://www.lures.info/childrens_search/gogooligans.html

https://www.factmonster.com/

http://cybersleuth-kids.com/

https://www.kidzsearch.com/sites.html

https://swiggle.org.uk/

https://primaryschoolict.com/

http://www.dibdabdoo.com/

https://www.britannica.com/

Ladybrook E-Safety and Computing Guidelines

- Use computing equipment responsibly, wash hands before you handle any iPad / laptops / computers / Chrome books.

- Ensure all computing equipment is put away and stored correctly – logout of computers and shut them down before storing them

- Ask permission before using the internet in school.

- Keep your personal Login information safe.
- Only access websites suggested by your teacher or that your teacher has said are suitable for you to access.

- If you are using the computer to communicate with others, be respectful and kind.

- Tell your teacher if you see something that is inappropriate or upsetting.