ROOTED IN GOD'S LOVE, EVERYONE GROWING TOGETHER TO BECOME THE BEST THAT WE CAN BE

Online Safety Policy

Policy Leader	Gemma Walker
Nominated Governor	Emma Huxley
Last Updated	September 2026
Approved by the Governing Body	14/10/2026
Date to Review	September 2027

At Barrow URC Primary School, we work hard to ensure that all of our pupils are included in all parts of school life. We begin with high quality teaching, ensuring that all of our staff are trained to support all children. For children with special educational needs or disability, we may make reasonable adjustments or call upon the support of external experts. We have high expectations for all of our children and track the progress they make carefully, ensuring timely and high quality intervention is in place where necessary. It is important that we work closely with families, with the child always at the heart of our approach. We provide a safe, inclusive environment, in which all children feel welcome and valued. In our school, the child is always at the heart of what we do. Our seven core values: Respect, Honesty, Trust, Love, Peace, Kindness and Forgiveness- are the pillars of our school community and help us to provide a safe, caring environment in which all our children feel welcome and valued.

BARROW U.R.C. PRIMARY SCHOOL

ROOTED IN GOD'S LOVE, EVERYONE GROWING TOGETHER
TO BECOME THE BEST THAT WE CAN BE

Contents

1. Purpose of this document
2. Roles and Responsibilities
3. Why internet use is important?
4. Staff and governor training
5. Teaching and Learning
6. Filtering and Monitoring
7. Network management and Cyber Security
8. Social Media, Online Communication and Personal Devices
   Online Abuse and Online Harms
9. Generative AI
10. Related Policies and Procedures

1. Purpose of this document



The purpose of this policy statement is to:

- Ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices.
- Provide staff and volunteers with the overarching principles that guide our approach to online safety.
- Ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.
- The policy statement applies to all staff, volunteers, children and young people and anyone involved in Barrow URC Primary School's activities.

2. Roles and Responsibilities

Role	Key Responsibilities
Headteacher Nicola McArdle	• To take overall responsibility for Online Safety provision • To take overall responsibility for data and data security (SIRO) • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements (Netsweeper) • 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) • To work with the online safety lead to regularly review Online Safety Policies and Practice using 360 Degree Safe

Online Safety Lead
Gemma Walker
 	
Designated Safeguarding Lead
Nicola McArdle
 	
Deputy Designated Safeguarding Leads
Helen Porter and Emily Rodriguez
 	
Online Safety Governor
Emma Huxley
	• Takes day to day responsibility for Online safety issues and has a leading role in establishing and reviewing the school Online safety policies / documents
	• Promotes an awareness and commitment to Online safeguarding throughout the school community
	• Ensures that Online safety education is embedded across the curriculum
	• Liaises with school computing technical staff
	• To communicate regularly with SLT and the designated Online safety Governor / 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 ensure that an Online safety incident log is kept up to date (Through CPOMs)
	• Facilitates training and advice for all staff
	• Liaises with the Local Authority and relevant agencies
	• Is 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 ○ online bullying and use of social media
Governors	• To ensure that the school follows all current Online safety advice to keep the children and staff safe • To approve the Online Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. • To support the school in encouraging parents and the wider community to become engaged in online safety activities • The role of the Governors will include: • To regular review with the Online Safety Lead (including Online safety incident logs, filtering / change control logs, CPOMs)
Computing Curriculum Leader Gemma Walker	• To oversee the delivery of the online safety element of the Computing curriculum • To liaise with the DSL regularly •
Network Manager/technician Nybble	• To report any online safety related issues that arise, to the Online safety Lead. • 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 IT system

	• To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices in line with GDPR regulations • The school's policy on web filtering is applied and updated on a regular basis • LGfL is informed of issues relating to the filtering applied by the Grid • That he / she keeps 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 • That the use of the network / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation. • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To keep up-to-date documentation of the school's online security and technical procedures.
Office Team Janis Smith, Fiona Stanley and Anne-Marie Brown	• To ensure that all data held on pupils on the school office machines have appropriate access controls in place
Lancashire Grid for Learning (LGfL) Nominated Contact(s)	• To ensure all LGfL services are managed on behalf of the school including maintaining the LGfL USO database of access accounts
All Staff	• To read, understand and help promote the school's online safety policies and guidance • To read, understand, sign and adhere to the school staff Acceptable Use Agreement

	• 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 Lead or DSL • 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 pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc
Pupils	• Read, understand, and adhere to the Pupil Acceptable Use Policy • 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
Digital Leaders	• To help the school in the creation/ review of online safety policies • To play an active role in the implementation of online safety in school • To model safe, responsible and professional behaviours in their own use of technology • To attend Online Safety meetings as part of the Barrow Online Safety Group
Parents/Carers	• To support the school in promoting online safety and endorse the pupils' use of the Internet and the school's use of photographic and video images • To read, understand and promote the school Pupil Acceptable Use Agreement with their children • To access the school website in accordance with the relevant school Acceptable Use Agreement. • To consult with the school if they have any concerns about their children's use of technology
External Groups	• Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the Internet within school

3. Why internet use is important?

We believe that:

- Children should be able to use the internet safely for both educational and personal development.
- In our modern world, the internet connects people together and opens students up to different ideas and cultures that they may not come into contact with on a regular basis.
- It provides children and young people with an abundance of resources for their learning
- It allows children to become digital literate which is important in Digital Britain.



We recognise that:

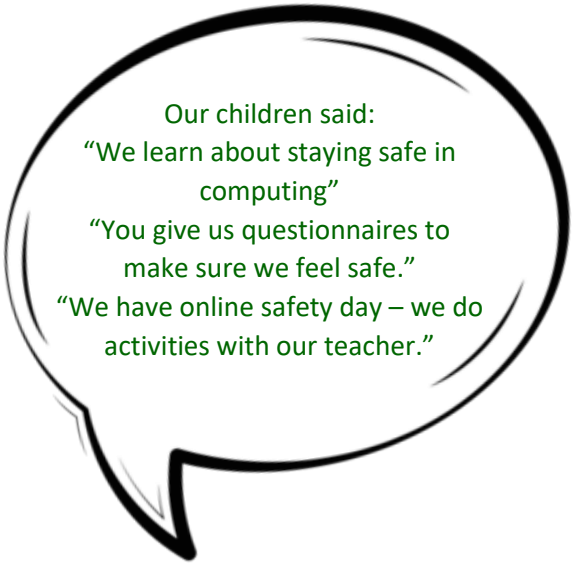
- the online world provides everyone with many opportunities; however it can also present risks and challenges
- we have a duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm online
- we have a responsibility to help keep children and young people safe online, whether or not they are using our school's network and devices all children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse
- working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety
- that Artificial Intelligence (AI) has the potential to enhance learning and innovation but also brings risks, such as privacy concerns and potential misuse, requiring careful management to ensure safe and responsible usage.

4. Staff and governor training

- Training is given to all staff and governors annually. This includes one session for staff and governors at the start of the year, a mid-yearly update as well as other updates when key issues or changes arise.
- Further training is arranged when incidents or issues arise

- All new staff [including those on university/college placement and work experience] are provided with information and guidance on the Online Safety policy and the school's Acceptable Use Policies as part of their induction process.
- Training will ensure that:
    - staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
    - staff know how to deliver Online Safety lessons to pupils effectively
    - staff are aware of new online safety issues and guidance

5. Teaching and Learning



- Online safety is taught as an embedded part of our curriculum through computing (KAPOW), PSHE (KAPOW) and in other relevant subjects, linking to other learning that is taking place.
- Online safety is also taught explicitly through half-termly online safety lessons at the end of each unit, with age-appropriate progression across the school.
- Where specific issues arise, additional teaching and learning will take place addressing that issue with the relevant year groups. Teaching will take account of pupils' age, developmental stage, SEND, EAL and individual vulnerabilities so that online safety education is accessible and meaningful for all pupils.

6. Filtering and Monitoring

- Filtering is a preventative safeguarding measure and monitoring is used to identify and respond to risks and incidents. The school will maintain appropriate filtering and monitoring systems that reflect the age, needs and risk profile of pupils and staff, including consideration of SEND, EAL and emerging technologies such as generative AI.

- The school uses educational filtered secure broadband connectivity through LGfL and the filtering provision currently in place. The named technical provider(s), filtering product(s), monitoring arrangements and escalation routes will be checked and recorded as part of the annual review.
- Filtering and monitoring provision is reviewed at least annually by the Senior Leadership Team, Designated Safeguarding Lead, IT/technical support and the Online Safety Governor. The review will consider effectiveness, coverage across devices and locations, pupil risk profiles, changes in technology, emerging threats, filtering gaps and any actions required.
- The school will ensure that filtering blocks harmful or inappropriate content while avoiding unreasonable restrictions on legitimate learning. Safe-search settings and age-appropriate access will be used where appropriate.
- Internet use is monitored and all users are informed of this. Staff and pupils must report suspected filtering or monitoring failures promptly to the Computing/Online Safety Lead or DSL. Technical staff will investigate, record and escalate issues to the relevant provider where necessary.
- Staff preview websites before use where appropriate and plan Internet use to match pupils' ability and learning needs. Child-friendly search tools and safe-search settings are used where appropriate, and particular vigilance is maintained when using image searches.
- Chat rooms, social networking and other high-risk services are blocked unless specifically required for an approved educational purpose and appropriately supervised. Access to external social media or other services for teaching purposes must be approved and risk assessed.
- All users are made aware of the rules for appropriate use, the monitoring arrangements and the consequences of misuse through the relevant Acceptable Use Agreements, staff training and the curriculum.
- Concerns involving harmful, illegal or inappropriate material are treated as safeguarding concerns where relevant. Suspected illegal content will be escalated to the DSL/Headteacher and, where appropriate, the police, Local Authority or other relevant agency in line with safeguarding procedures.
- Filtering and monitoring logs, incidents, actions and changes will be retained so that the school can evidence its review and response arrangements. The Online Safety Lead will review incident and filtering/change-control information with the DSL and technical staff.
- The school will test filtering and monitoring arrangements following significant changes, incidents or the introduction of new technology, including generative AI tools, and will document any remedial action.

- **Network management and cyber security**

- The school will maintain appropriate cyber security measures, including malware protection, secure configuration, access controls, software updates, backups and recovery arrangements.
- Staff will receive appropriate guidance on phishing, suspicious links, malicious attachments, passwords, multi-factor authentication where available, and reporting suspected cyber incidents.
- Suspected cyber security incidents, loss of devices or data breaches will be reported promptly to the Headteacher/appropriate data protection lead and managed under the school's incident response procedures.
- The school will review cyber security arrangements regularly and consider relevant DfE and National Cyber Security Centre guidance.

Barrow URC Primary School:

- Uses individual, audited log-ins for all staff
- Uses guest accounts occasionally for external or short term visitors for temporary access to appropriate services
- Ensures the Systems Administrator / network manager is up-to-date with LGfL services and policies / requires the Technical Support Provider to be up-to-date with LGfL services and policies;
- Storage and processing of personal data will comply with current UK data protection law and the school's data protection procedures. The school will not rely on the former EU Data Protection Directive wording. Any online service used to process pupil or staff data must be appropriately assessed and approved.

- **Password policy**

Barrow URC Primary School:

- makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it;
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.

- **E-mail**

Barrow URC Primary School:

- Provides staff with an email account for their professional use, LA email and makes clear personal email should be through a separate account;
- Does not publish personal e-mail addresses of pupils or staff on the school website.
- Will ensure that email accounts are maintained and up to date
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.

- Knows that spam, phishing and virus attachments can make e mails dangerous. We use a number of LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language. , Finally, and in support of these, Netsweeper filtering monitors and protects our Internet access to the World Wide Web.
- Pupils are taught about the online safety and 'netiquette' of using e-mail both in school
- Staff can only use LA or LGfL e-mail systems for professional purposes
- Access in school to external personal email accounts may be blocked
- Staff use a 'closed' LA email system which is used for LA communications and some 'LA approved' transfers of information
- Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper and that it should follow the school 'house-style':
- the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used;
- the sending of chain letters is not permitted;
- o embedding adverts is not allowed

- **Social Media, Online Communication and Personal Devices**
  - School staff must not use personal social media accounts to communicate with pupils or create online spaces for pupils using personal accounts. Digital communication with pupils must use school-approved systems and must remain professional and appropriate.
  - Staff should not post or share confidential or identifying information about pupils, parents/carers or colleagues, or content that could reasonably damage trust in the school. Staff should maintain appropriate privacy and security settings on personal accounts.
  - Any school social media account must have clear ownership, appropriate access controls and a defined purpose. Content should be monitored and managed in line with school procedures.
  - Online incidents involving pupils, staff or families should be reported to the DSL/Online Safety Lead where they may present a safeguarding, bullying, wellbeing or professional conduct concern.
  - CCTV is used in school for site surveillance and safety. Recordings are retained by the Support Provider for 28 days, subject to the school's data protection and CCTV procedures, and may be disclosed to the police or other lawful authority where appropriate.
  - Children's personal devices: if phones are brought into school by children, they must be taken to the office at the start of the day and cannot be collected until the end of the day. Phones must be turned off while in school.
  - Smart watches and other connected devices must be on aeroplane mode or otherwise disabled from communications/recording functions while in school, unless an agreed reasonable adjustment or safeguarding arrangement applies.
  - Other personal devices, including tablets, cameras and gaming devices, must only be used in school with permission and in accordance with the relevant Acceptable Use, safeguarding and image-sharing procedures.

7. School Website

- The Headteacher takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Uploading of information is restricted to our website authorisers: school administrator and school technician.
- The school web site complies with the statutory DfE guidelines for publications;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the school address, telephone number and we use a general email contact address, e.g. office@barrow.lancs.sch.uk or head@barrow.lancs.sch.uk

- Home information or individual e-mail identities will not be published
- Photographs published of children on the web do not have full names attached
- All photographs published of pupils have permission from parents/carers
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website
- We do not use embedded geodata in respect of stored images
- We expect teachers using' school approved blogs or wikis to password protect them and run from the school website.

8. Generative AI

- The school recognises that generative AI can support teaching, learning and administration but can also create safeguarding, privacy, accuracy, intellectual property, bias, manipulation and cyber security risks. Any use of AI must support the school's safeguarding responsibilities and wider data protection requirements.
- Pupils will only use generative AI tools where the school has approved the tool, considered the age restrictions and risks, and put appropriate supervision, filtering and monitoring safeguards in place. Pupils will not be required to create accounts on age-restricted services or enter personal, sensitive or confidential information into AI tools.
- Staff may use generative AI only in line with school-approved arrangements. Staff must not enter personal, special category, confidential or otherwise sensitive information about pupils, families or colleagues into public AI tools unless the use has been specifically approved and appropriate safeguards are in place.
- Where AI-generated content is used, staff and pupils should consider whether it is accurate, biased, suitable and appropriate for the intended purpose. Pupils will be taught that AI-generated material may be incorrect or misleading and that they remain responsible for checking and evaluating information.
- The school will consider the risks of AI-generated images, audio or video, including impersonation, manipulated content, deepfakes, bullying and reputational harm. Concerns about harmful AI-generated content will be reported and managed as safeguarding concerns where appropriate.
- AI tools used by the school will be subject to appropriate procurement, data protection, safeguarding, filtering and monitoring checks. The school will review AI arrangements as part of its online safety and filtering/monitoring reviews.

9. Online Abuse and Online Harms

- Online abuse can include grooming, sexual abuse or exploitation, coercive or controlling behaviour, harassment, threats, hate or discriminatory abuse, image-based abuse, sharing of

private information, impersonation, scams, exploitation through gaming or live-streaming, and other harmful contact or content.

- Online bullying is bullying that takes place over digital devices such as mobile phones, computers, tablets and games consoles. It may involve messages, apps, social media, forums or gaming platforms and can include harmful, false or humiliating content or sharing private information.
- Any concern that a child may be experiencing or causing harm online must be reported promptly to the DSL or a DDSL and recorded through the school's safeguarding/incident recording system. Staff must follow the school safeguarding procedures and must not investigate beyond their role or promise confidentiality.
- Where an online incident may constitute a criminal offence or serious safeguarding concern, the DSL/Headteacher will consider referral to children's social care, the police, Local Authority or other relevant agencies in line with safeguarding procedures.
- Pupils are taught how to block or report users, preserve evidence where appropriate, seek help from a trusted adult and use school reporting routes. Parents/carers are encouraged to contact the school where an online concern affects a child's safety, wellbeing or education.

10. Related Policies and Procedures

- Online safety concerns will be managed within the school's wider safeguarding framework. This policy does not replace the school's safeguarding policy or procedures.
- This policy should be read alongside:
    - Safeguarding Policy and procedures
    - Procedures for responding to concerns about a child or young person's wellbeing
    - Procedures for dealing with allegations of abuse made against a child or young person
    - Managing allegations against staff and volunteers
    - Code of Conduct for staff and volunteers
    - Anti-Bullying Policy and procedures
    - Photography and image sharing guidance
    - Acceptable Use Agreements and relevant mobile/device procedures