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

ONLINONLINE SAFETY POLICY

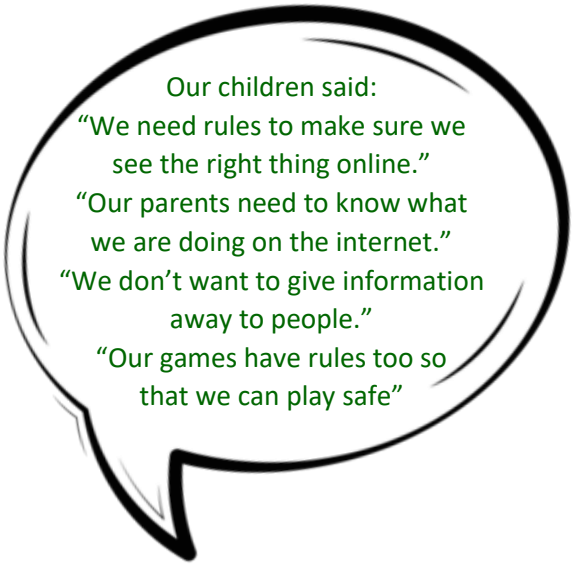
Policy Leader	Gemma Walker
Nominated Governor	Emma Huxley
Last Updated	March 2025
Approved by the Governing Body	March 2025
Date to Review	July 2026

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.

Contents

1. Purpose of this document
2. Roles and Responsibilities
3. Why internet use important?
4. Staff and governor training
5. Teaching and Learning
6. Internet Security
7. School Website
8. Online bullying
9. Related Procedures and Policies

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 **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: o sharing of personal data o access to illegal / inappropriate materials o 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:

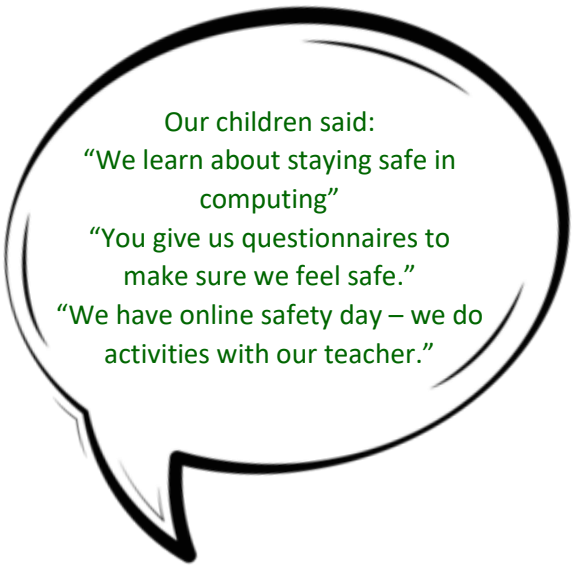
- the online world provides everyone with many opportunities; however it can also present risks and challenges
- we have a duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm online
- we have a responsibility to help keep children and 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 in discreetly through half-termly online safety lessons at the end of each unit.
- Where specific issues arise, additional teaching and learning will take place addressing that issue with the relevant year groups.

6. Internet Security

- **Internet access, security (virus protection) and filtering**
  This school:
  - Has the educational filtered secure broadband connectivity through the LGfL and so connects to the 'private' National Education Network;
  - Uses the LGfL filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc.
  - Uses USO user-level filtering where relevant, thereby closing down or opening up options appropriate to the age / stage of the students;
  - Ensures network health through use of Sophos anti-virus software (from LGfL) etc. and network set-up so staff and pupils cannot download executable files;
  - Uses LA approved systems secured email to send personal data over the Internet and uses encrypted devices or secure remote access were staff need to access personal level data off-site;

- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons;
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level
- Works in partnership with the LGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students;
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies where pupils have more flexible access;
- Requires staff to preview websites before use [where not previously viewed or cached] and encourages use of the school's Learning Platform as a key way to direct students to age / subject appropriate web sites; Plans the curriculum context for Internet use to match pupils' ability, using child-friendly search engines where more open Internet searching is required; e.g. yahoo for kids or ask for kids , Google Safe Search
- Is vigilant when conducting 'raw' image search with pupils e.g. Google image search;
- Informs all users that Internet use is monitored;
- Informs staff and students that that they must report any failure of the filtering systems directly to the Computing Subject Leader. Our system administrator logs or escalates as appropriate to the Technical service provider or LGfL Helpdesk as necessary;
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;
- Provides advice and information on reporting offensive materials, abuse/ bullying etc. available for pupils, staff and parents o Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.
- The DSL/Head Teacher receives information about the top 10 websites denied and allowed from BT Lancashire.

- **Network management (user access, backup)**

  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 of all data within the school will conform to the UK data protection requirements Pupils and Staff using mobile technology, where storage of data is

online, will conform to the EU data protection directive where storage is hosted within the EU.

- **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 networking**
  - Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students.
  - School staff will ensure that in private use:
    - No reference should be made in social media to students / 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.

- **CCTV**
  - We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings (retained by the Support Provider for 28 days), without permission except where disclosed to the Police as part of a criminal investigation.

- **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 must be on aeroplane mode at all times while in school.

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. Online Abuse

- Online bullying is bullying that takes place over digital devices like mobile phones, computers, tablets and game consoles. Online bullying can occur through SMS and apps, or online in social media, forums, or gaming where people can view, participate in, or share content. Online bullying includes sending, posting, or sharing negative, harmful, false, or mean content about someone else. It can include sharing of personal or private information about someone else causing embarrassment or humiliation. Some online bullying crosses the line into unlawful or criminal behavior. (What Is cyber bullying, Gov.Uk, 2022)
- Barrow URC Primary Anti-Bullying Policy can be accessed through the school's website.

9. Related Policies and Procedures

This policy statement should be read alongside our organisational policies and procedures, including:

- safeguarding
- procedures for responding to concerns about a child or young person's wellbeing
- 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.