Royles Brook Primary School

Online Safety Policy 2024-2025

Policy Version & Issue Date	V1.0 September 2024
Date of next review	September 2025
Person responsible for Review	J. McKinnon

Online Safety Policy

This Online Safety Policy has been written as part of a consultation process involving the following people through annual Safeguarding Training completed by all staff and governors:

Headteacher, Computing Coordinator, Teachers, Support Staff, Office Staff, IT technician and governors

Introduction

This policy applies to all members of the school community, including staff, pupils, parents/carers, visitors and school community users.

Research has proven that use of technology brings enormous benefits to learning and teaching. However, as with many developments in the modern age, it also brings an element of risk. Whilst it is unrealistic to eliminate all risks associated with technology, the implementation of an effective Online Safety Policy will help children to develop the knowledge, skills and confidence to manage potential risks and considerably reduce their impact.

Our Online Safety Policy, as part of the wider safeguarding agenda, outlines how we will ensure that our school community is prepared to deal with the safety challenges that the use of technology brings. The policy is organised in 4 main sections:

- Policies and Practices
- Infrastructure and Technology
- Education and Training
- Standards and Inspection.

Royles Brook Primary School Vision for Online Safety:

At Royles Brook Primary School, we use information technology when appropriate, to enhance learning opportunities for our children and to support daily organisation and administrative tasks carried out by school staff.

Keeping members of our school community safe, whilst using information technology, is a priority and we expect staff to act as role models in their use of technology and abide by the shared decisions reflected in our Online Safety Policy. Children are encouraged to explore and make responsible decisions regarding their uses of technology, informed by 'education' as opposed to the imposition of restrictions. As children are engaging with 21st Century technologies both inside and outside of school, we will provide opportunities for both children and the wider community to understand and view Online Safety education as a key life skill.

Our Online Safety Policy defines what we consider to be acceptable and unacceptable behaviour regarding the uses of technology in school and the sanctions or procedures to be followed should breaches of security occur. The policy is communicated to all staff, governors, pupils and parents/carers and is updated in light of the introduction of new technologies or incidents.

<u>The role of the school's Online Safety Champion:</u>

The Headteacher is the Online Safety Champion and also the DSL. Some aspects of the role are now undertaken by the SLT and the Computing Coordinator.

The role will include:

- To ensure that all documents linked to the Online Safety Policy including Acceptable User Policies are kept up to date.
- Continue to monitor and ensure that all staff adhere to the Online Safety Policy.
- Ensure that all staff are aware of the reporting procedures and requirements should an Online Safety incident occur.
- Ensure the Online Safety incident log is appropriately maintained and regularly reviewed.
- Keep up-to-date with Online Safety issues and guidance through liaison with the Local Authority Schools' ICT Team and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP).
- Provide or arrange Online Safety advice/training for staff, parents/carers and governors.
- Ensure the SLT, staff, pupils and governors are updated as necessary.

<u>Policies and practices:</u>

This Online Safety Policy should be read in conjunction with the following other related policies and documents:

Behaviour Policy

Staff Code of Conduct

Safeguarding and Child Protection Policy

Acceptable Use Policy

Security and Data Management

In our school, data is kept secure and all staff are informed as to what they can/cannot do with regard to data in the following ways:

- Key information/data is mapped and securely stored on the Main Office computer. This is accessible only by the Office Staff and Headteacher.
- The Headteacher has overall responsibility for managing all information.
- Staff have been informed of the location of all data relevant to them by the Headteacher/ Office Staff/ SLT and Computing Coordinator.
- Staff have been informed of their legal responsibilities with respect to principles of the Data Protection Act (1988) and ensure all data is:
    1. Accurate
    2. Secure
    3. Fairly and lawfully processed
    4. Processed for limited purposes
    5. Processed in accordance with the data subject's rights
    6. Adequate, relevant and not excessive
    7. Kept no longer than necessary
    8. Only transferred to others with adequate protection; sensitive data to be sent electronically using encrypted messaging only

Our school ensures that data is appropriately managed both within and outside the school in the following ways:

- School's equipment, including teacher laptops, must only be used for school purposes and do not contain personal information e.g. personal images, personal financial details, music downloads, personal software. Computers are accessed via a safe username and password and it is the responsibility of the individual to keep this secure at all times. Any breaches in security must be reported immediately to the Headteacher.
- School equipment must not be used, for example for online gambling, dating websites, home shopping, booking holidays, and social networking both at home and in school.
- Staff are aware of the school's procedures for disposing of sensitive data, e.g. shredding hardcopies, deleting digital information, deleting usernames and passwords from school's VLE, deleting email accounts, IEP, PIPs, SATs information and know the person responsible should there be any queries. Also see Disposal of Assets, Internal Financial Regulations

- The school's policy for removal of sensitive data prior to disposal or repair of equipment is documented in The ICT Security Framework and all staff are aware of the person responsible. In our school this is Miss S. Uttley, School Business Manager.
- Remote access is available to staff and they are only allowed to access data from home via a secured wireless connection. School data must not be stored on personal equipment, e.g. home computer or mobile phone.
- Each member of staff has been provided with a password protected laptop/IPad to store data as part of their professional role e.g. writing or backing up reports or IEPs. All staff have access to a personal storage space on the server and a shared space on Microsoft One Drive, and should use these as the preferred area for backing up data.

Use of mobile devices:

In our school we recognise that the use of mobile devices could offer a range of opportunities to extend children's learning. However, the following statements must be considered when using these devices:

- No use of mobile phones, when working with children, unless agreed by a member of the Senior Leadership Team/DSL.

- No data to be stored on mobile phones directly linked to children's' details.

Use of digital media:

In our school we are aware of the issues surrounding the use of digital media online. All members of our school understand these issues and should ensure that any use of digital media is inline with our school's Safeguarding and Child Protection Policy and maintains staff's Professional Code of Conduct. In addition:

- Consent must be sought before any individual, within the school, appears in any media.

- Consent from parents/carers will be obtained as part of the induction process.

- Time period of retaining pictures after a child has left the school is 1 year.

- Full names will not be used in connection with digital media.

- Pictures must not be posted on social network sites by staff. They can only be posted on school sites with the permission of parents/carers.

- All photographs should be held centrally on the Shared Drive.

- Staff must ensure photographs taken are appropriate and children are dressed appropriately.

- Permission must be sought before posting any pictures on social networks or the internet from the Headteacher.

All these points are monitored by the Online Safety champion.

Communication technologies:

Keeping Children Safe in Education 2023 states that

'Schools and colleges are likely to be in regular contact with parents and carers. Those communications should be used to reinforce the importance of children being safe online and parents and carers are likely to find it helpful to understand what systems schools and colleges use to filter and monitor online use. It will be especially important for parents and carers to be aware of what their children are being asked to do online, including the sites they will asked to access and be clear who from the school or college (if anyone) their child is going to be interacting with online.'

Email:

In our school the following statements reflect our practice in the use of email:

- Emailing should only be done to and from lancsngfl email accounts.

- When communicating with outside groups this should still be done from the lancsngfl account and if data or confidential information is to be shared, the email must be encrypted.

- Inappropriate e-mail issues and incidents should be reported to the Headteacher.

Social Networks:

In our school, the following statements outline what we consider to be acceptable and unacceptable use of Social Network sites:

- There should be no accessing of personal social networks on school equipment.

- Staff are strongly advised to avoid putting personal information/photos on social networking sites which parents and children can access.

Mobile telephone and Smart watches:

- Staff must not use their mobile phones when working with children and must never use them as a camera.

- Staff must not use their smart watches (other than to tell the time) when working with children.

- Staff have to be aware of how to monitor these systems, including usage by specific children.

Websites and other online publications:

In our school, the following statements outline what we consider to be acceptable and unacceptable use of websites and other online publications:

- All people involved in creating digital media have to be aware of the guidance.

- All people to be aware of what personal information is allowed on the website.

- Access and editing of the website is done by the Headteacher, Computing Lead and School Business Manager.

- The Headteacher has overall responsibility for the content on the website.

- Any copyright restrictions should be adhered to when placing content on the website.

- The information on the website should be available for everyone to see.

- All documents should be read only format so that they cannot be altered by other parties.

Video conferencing:

In our school the following statements outline what we consider to be acceptable and unacceptable use of video conferencing:

- We utilise secure video conferencing facilities including Zoom, Microsoft Teams and Google Meet.

Acceptable Use Policy:

All staff and pupils must adhere to this policy which works in conjunction with this policy.

Dealing with incidents:

Illegal Offences

Any suspected illegal material or activity must be brought to the immediate attention of the Headteacher who will refer this to external authorities. Never personally investigate, interfere with or share evidence as you may inadvertently be committing an illegal offence. Illegal content will be reported to the Internet Watch Foundation http://www.iwf.org.uk.

Illegal content includes:

Child sexual abuse images

- Criminally obscene adult content
- Incitement to racial hatred

Inappropriate Use

This is much more likely and any incidents must be dealt with quickly and actions chosen which are proportionate to the offence.

Incident	**Procedure and Sanctions**
Accidental access to inappropriate materials	Minimise the web page; turn off the monito Tell a trusted adult Enter the details in the Incident Log Persistent 'accidental' offenders would be subject to disciplinary action
Using other people's logins and passwords maliciously	Inform SLT or designated Online Safety Champion Enter the details in the Incident Log Additional awareness raising of Online Safety issues and the Acceptable Use Policy with individual child/class More serious or persistent offences may result in further disciplinary action Parents/Carers informed
Deliberate searching for inappropriate materials	
Bringing inappropriate electronic files from home	
Using chats and forums in an inappropriate way	

Infrastructure and technology:

Pupil Access:

This is done on an individual basis in all classes.

Passwords:

These are individual login details for children in Key Stage 1 and Key Stage 2. Children in EYFS are logged into programs by school staff.

Staff Access:

This is done on an individual basis.

Passwords:

These are individual passwords.

Administrator Access:

This is kept by the Headteacher and School Business Manager and the IT technicians.

Passwords:

These are individual passwords.

All staff and pupils are aware of the importance of keeping passwords secure. All staff and pupils have to raise an issue with the Headteacher for passwords to be changed or renewed. Passwords need to be changed regularly to ensure security.

Software/hardware:

- All software has to be legally owned to be placed on the intranet.
- All licences are held centrally in the office.
- All equipment is audited annually.
- Software should only be placed on the intranet by the IT technician, who should notify the Computing Coordinator and the Online Safety Champion.
- Teachers can place software on their own school laptops to assess the quality of it, however, they are discouraged from doing so and any software to be used on a regular basis must be

installed on the Server. This can only be carried out by the Technician or Computing Coordinator.

Managing the network and technical support:

- The server is held securely in a locked cupboard/ICT Suite and is accessed by the Headteacher, School Business Manager, Computing Coordinator and IT Technician.
- All wireless devices are password protected

Security of the school system is monitored by the IT Technician and overseen by the Computing Coordinator and Headteacher.

- The security and safety of the system is monitored regularly by the IT Technician and the Computing Coordinator.
- Critical updates are installed when they are sent by software providers.
- Teachers and pupils have access to the intranet by usernames and passwords.
- Staff and pupils are expected to logout of their computers when leaving them unattended.
- The IT technician, with support of the Computing Coordinator, are central points to report incidents of breach of security.
- School equipment must not be used for any purpose other than school business e.g. no personal internet use, e-mail use, no storage of personal photos.
- All technicians are aware of our school policies.
- The Computing Coordinator is responsible for coordinating and discussing issues with the technicians.

Filtering and Monitoring:

The Headteacher is responsible for:

- procuring filtering and monitoring systems
- documenting decisions on what is blocked or allowed and why
- reviewing the effectiveness of your provision
- overseeing reports

They are also responsible for making sure that all staff:

- understand their role
- are appropriately trained
- follow policies, processes and procedures
- act on reports and concerns

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL should work closely together with IT service providers to meet the needs of your setting. You may need to ask filtering or monitoring providers for system specific training and support.

The DSL should take lead responsibility for safeguarding and online safety, which could include overseeing and acting on:

- filtering and monitoring reports
- safeguarding concerns
- checks to filtering and monitoring systems

The IT service provider should have technical responsibility for:

- maintaining filtering and monitoring systems
- providing filtering and monitoring reports
- completing actions following concerns or checks to systems

The IT service provider should work with the Headteacher and DSL to:

- procure systems
- identify risk
- carry out reviews
- carry out checks

At Royles Brook Primary School, the following is carried out to ensure we are able to safeguard all children:

- Filtering is carried out by using Securus Software.

- Instantly, the Headteacher, DSLs and IT Technician receive alerts to any potential breaches via Securus. The alert is thoroughly checked and appropriate actions taken if an inappropriate search has been carried out.

- Termly Filtering tests to ensure that the following content is blocked:

Child Sexual Abuse Content

Terrorism Content

Adult Content

Offensive Language

No child is allowed to use any school device unsupervised. When carrying out work on electronic devices with access to the internet, staff must monitor what children are using by positioning themselves within the classroom so that they can see what is being accessed.

- All staff receive appropriate training as part of their annual safeguarding training to ensure they understand how to monitor children's use of devices/the internet. They sign to agree they have received this training and understand their role in keeping children safe when using devices/the internet.

<u>Education and Training:</u>

Online Safety across the curriculum:

- This is taught each term through our Computing Curriculum to individual classes and to the whole school via Assemblies.

<u>Online Safety – Raising parents/carers awareness:</u>

Ways to keep children safe online is communicated by the Headteacher/DSLs to carers and parents through the following resources:

- Monthly Online Safety Guides.
- The links to a wide range of websites containing advice and support is added to the school website and maintained regularly.

<u>Standards and inspection:</u>

We will know as a school, if Online Safety is having the desired effect through closely monitoring activities by the Online Safety Champion, regular meetings with all interested parties and analysis of Online Safety incidents.

Online Safety incidents are reported to the Headteacher, and when they occur, are reported in the Headteacher's Termly Report to governors.

New technologies are to be risk assessed before they are implemented by the IT technicians with the involvement of the Headteacher and the Computing Coordinator.

Incident books are held with the Headteacher to record issues and problems with the software and hardware in the school. These should be analysed by the IT Technician and Computing Coordinator to ensure that patterns and recurring incidents are eliminated by talking and working with specific groups.

The documents related to Online Safety will have to be changed according to the issues raised.

Any document changes will have to be reported to the Headteacher, staff, governors, parents and children as deemed appropriate by the Online Safety Champion.

Acceptable Use Policies should be created at the time of admission and updated if new technologies are implemented.