Developing and Reviewing this Policy

This Online Safety Policy has been written as part of a consultation process involving the following people:

Staff at Rosegrove Infant School and Rosegrove Nursery School and written in light of Lancashire Guidance.

It has been approved by Governors and will be monitored and reviewed as listed below:

Policy Created – October 2016

Reviewed – October 2017

The implementation of this policy will be monitored by Mrs L Renshaw/Mrs C Ashworth

This policy will be reviewed annually by Mrs L Renshaw/Mrs C Ashworth

Introduction

This policy applies to all members of the school community (including staff, pupils, parents/carers, visitors, including students 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 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 our school community are 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.

1. Our school's vision for Online Safety

The purpose of Internet access in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration system. Access to the Internet is a necessary tool for staff and an entitlement for students.

2. The role of the school's Online Safety Champion

Our Online Safety Champion is Mrs C Ashworth

The role of the Online Safety Champion in our school includes:

- Having operational responsibility for ensuring the development, maintenance and review of the school's Online Safety Policy and associated documents, including Acceptable Use Policies.
- Ensuring that the policy is implemented and that compliance with the policy is actively monitored.

- Ensuring all staff are aware of reporting procedures and requirements should an Online Safety incident occur.
- Ensuring the Online Safety Incident Log is appropriately maintained and regularly reviewed.
- Keeping personally 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).
- Providing or arranging Online Safety advice/training for staff, parents/carers and governors.
- Ensuring the Headteacher, SLT, staff, pupils, Governors and volunteers are updated as necessary.
- Liaising closely with the school's Designated Senior Leader to ensure a co-ordinated approach across relevant safeguarding areas.

3. Policies and practices

The Online Safety policy should be read in conjunction with the following policies/documents:-

School Improvement Plan, Staff Code of Conduct, Acceptable Use Policies,

Recruitment and Induction Procedures, Safeguarding and Child Protection Policy,

Lancashire County Council ICT Security Framework for Schools.

4.1 Security and data management

In line with the requirements of the Data Protection Act (1998), sensitive or personal data is recorded, processed, transferred and made available for access in school. This data must be:

- Accurate
- Secure
- Fairly and lawfully processed
- Processed for limited purposes
- Processed in accordance with the data subject's rights
- Adequate, relevant and not excessive

- Kept no longer than is necessary
- Only transferred to others with adequate protection.

All data in school must be kept secure and staff informed of what they can or can't do with data through the Online Safety Policy and statements in the Acceptable Use Policy (AUP).

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:

- Devices containing data should only be removed from school with the specific permission of the Headteacher.
- All devices should be password protected and staff are expected to keep this data secure and delete when no longer needed.
- If a member of staff loses any removable device this must be reported immediately to the Headteacher.

Access eligibility will be reviewed continually. In particular the relevant access capability will be removed when a person leaves the employment of the school. In addition, access codes, user identification codes and authorisation rules will be reviewed whenever a user changed duties.

Backups

In order to ensure that our essential services and facilities are restored as quickly as possible following an ICT system failure, back-up copies of stored data will be taken at regular intervals as determined by the System Manager, dependent upon the importance and quantity of the data concerned

Security copies should be clearly marked as to what they are and when they were taken and stored away from the system to which they relate in a restricted access fireproof location and/or off site.

Security copies should be regularly tested to ensure that they enable the systems/relevant file to be re-loaded in cases of system failure.

Disposal of Waste

Disposal of waste ICT media will be made with due regard to the sensitivity of the information they contain. For example, paper will be shredded if any confidential information from it could be derived.

> *The Data Protection Act requires that adequate mechanisms be used when disposing of personal data.*

Disposal of Equipment

Prior to the transfer or disposal of any ICT equipment the System Manager must ensure that any personal data or software is obliterated from the machine if the recipient organisation is not authorised to receive the data. The Schools' ICT Group recommend the use of Preston Recycling 01772 562411 to support in the process of removing data if required. Where the recipient organisation is authorised to receive the data, they must be made aware of the existence of any personal data to enable the requirements of the Data Protection Act to be met. Normal write-off rules as stated in Financial Regulations apply.

> *The Data Protection Act requires that any personal data held on such a machine be destroyed.*
>
> *It is important to ensure that any copies of the software remaining on a machine being relinquished are legitimate. Care should be taken to avoid infringing software and data copyright and licensing restrictions by supplying unlicensed copies of software inadvertently.*

4.2 Use of mobile devices

Many mobile phones have inbuilt cameras. Support staff's mobile phones are not allowed to be used in class and must be kept in staff lockers during the working day (this does not include breaks). Teachers must keep their mobile phones in their classroom in case of emergencies but are not permitted to use them in the presence of children. If staff are waiting for an urgent call they must inform the Headteacher of the need to use their mobile phone during session time and arrangements will be made for a call to be taken out of the classroom. The site supervisor may keep his phone with him (Health and Safety risk assessment on lone working) and can use his phone but not in the presence of children. Mobile phones must only be used in the staff room or main office if pupils are in the building.

Cameras, mobile phones and other recording devices are prohibited in all toilet and changing areas.

Please also see information in the Safeguarding and Child Protection Policy and the Acceptable Use of ICT Policy

4.3 Use of digital media

Children have their photographs taken to provide evidence of their achievements for developmental records and also in relation to school events and to promote the school. Staff, visitors, volunteers and students are not permitted to use their own mobile phones to take or record any images of children for their own records under any circumstances.

Procedures

- Under the Data Protection Act 1998, the school seeks parental consent to take photographs and use video recorders. Photographs will be stored on staff laptops which are password protected. Photographs are deleted one term after the children leave our school.
- The school's digital cameras or memory cards must not leave the school setting unless on an official school trip. Photographs are printed/uploaded in the setting by staff and once done images are removed from the cameras memory.

Photographs may be taken anywhere in the school grounds or of pupils out of school on a supervised visit/trip. Often photographs may contain other children in the background. These photographs may form part of a learning journey but digital images will not be shared.

Parents are not allowed to use their mobile phone in school. The school will take photographs of children to give to parents if requested during school visits / open days. The school concerts are videoed and copies are sold. Parents are asked for permission before their child is recorded.

Under the Data Protection Act (1998), parents are entitled to take photographs of their own children on the provision that the images are for their own use. Including other children or other purpose could constitute a potential breach of Data Protection legislation.

Recognisable photographs may be used on the school website, Twitter page or any school advertising/promotional documents. Parents are asked permission before external photographers take photographs, for example, to use in the newspaper.

4.4 Communication technologies

Email:

The use of e-mail in school

Pupils will not have individual e-mail accounts that can be accessed outside of school. They will be able to access an e-mail program that allows them to email other members of the class within the school setting. Staff are aware that any e-mails sent are like sending a letter on schools headed notepaper and that only appropriate language will be used.

The following statements reflect our practice in the use of email.

- All users have access to the Microsoft online Office 365 service as the preferred school e-mail system.
- Only official email addresses should be used to contact staff.

- All users are aware of the risks of accessing content including SPAM, unsuitable materials and viruses from external email accounts, e.g. Hotmail or Gmail, in school.
- All users are aware that email is covered by The Data Protection Act (1988) and the Freedom of Information Act (2000), meaning that safe practice should be followed in respect of record keeping and security.
- All users are aware that all e-mail communications may be monitored at any time.
- All user must immediately report any e-mail that makes them feel uncomfortable, is offensive, threatening or bullying in nature. They must not respond to any such communication but report it to the e-safety champion.

Social Networks:

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

Employees who choose to make use of social networking site/media are advised as follows:

- That they familiarise themselves with the sites 'privacy settings' in order to ensure that information is not automatically shared with a wider audience than intended;
- That they do not conduct or portray themselves in a manner which may;-

  Bring the school into disrepute

  Lead to valid parental complaints

  Be deemed as derogatory towards the school and/or it's employees

  Be deemed as derogatory towards pupils and/or parents and carers

  Bring into question their appropriateness to work with children and young people.

- That they do not form on-line 'friendships' or enter into communications with parents/carers and pupils as this could lead to professional relationships being compromised.
- On-line friendships and communication with former pupils should be strongly discouraged particularly if the pupils are under the age of 18
- Photographs and comments made on the Twitter feed are only posted by designated staff. The page is monitored by the Head teacher and 'School's Social Media'

Mobile telephone:

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

- Pupils do not have mobile phones in school
- Staff are allowed to use personal mobile phones in designated areas of school, but this must not interfere with their supervision of pupils. (also see Child Protection Policy)
- Staff use personal mobile phones as a means of contact when on school trips.
- Mobile phones are not used to support lessons.

Instant Messaging:

The Lancashire Lightspeed Filtering service 'blocks' these sites and they are not used in school.

Virtual Learning Environment (VLE) / Learning Platform:

In our school the following statements outline what we consider to be acceptable and unacceptable use of Virtual Learning Environments:

- Passwords are issued and their security maintained.
- Accounts are deleted when staff and pupils leave the school. This is monitored by the Online Safety Champion/Headteacher.

Web sites 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:

The school website is edited by the Schools ICT technician under the guidance of the Headteacher. The Headteacher has overall responsibility for what appears on the web site. Downloadable materials will be in 'read only' format to prevent content being manipulated and potentially re distributed without the school's consent.

Video conferencing:

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

- Parents are asked to sign to give permission for their child/children to participate in video and photographs when they first start school.
- Approval by the Headteacher must be obtained in advance of the video conference taking place. All sessions should be logged including the date, time and the name of the external organisation/ person(s) taking part.
- Pupils using video conferencing equipment should be supervised at all times. All staff supervising video conferencing equipment should know the procedures to follow if they are unhappy with the content of a VC session e.g. how to, stop or hang up the call.
- Copyright, privacy and Intellectual Property Rights (IPR) legislation will be breached if images, video or sound are recorded without permission.
- Recordings will not be used for any other purpose than that originally agreed.

Others:

School will need to adapt/update this policy in the light of emerging new technologies and any issues or risks associated with these technologies.

4.5 Acceptable Use Policy (AUP)

An Acceptable Use Policy ensures that all users of technology within school will be responsible and stay safe.

4.6 Dealing with incidents

All suspected illegal material or activity must be brought to the immediate attention of the Headteacher who must refer this to the appropriate external authority e.g. Police, CEOP, Internet Watch Foundation (IWF)

Incident	Procedure and Sanctions
Accidental access to inappropriate materials	• Activate Hector/turn the mobile device off. • Tell a trusted adult. • Enter the details in the Incident Log and report to LGfL filtering services if

	necessary. • Persistent 'accidental' offenders may need further disciplinary action.
Using other peoples' 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 AUP with individual child/class/member of staff. • More Serious or persistent offences may result in further disciplinary action. • Consider parent/carer involvement.
Deliberate searching for inappropriate materials.	
Bringing inappropriate electronic files from home.	
Using chats and forums in an inappropriate way.	

5. Infrastructure and technology

Rosegrove Infant School subscribes to the lightspeed filtering service and internet content filtering is provided through this. It is important to note that the filtering service offers a high level of protection but occasionally unsuitable content may get past the filter service. Sophos Anti-Virus software is included in the school's subscription, but this needs to be installed on computers in school and then configured to receive regular updates. Further information can be found at www.lancsngfl.ac.uk/eSafety .

Pupil Access:

- Pupils are supervised at all times when accessing school equipment and online materials.

Passwords:

- Passwords are in place on computers accessed by pupils. Staff are issued with secure username and passwords. Administrator passwords for the school network are issued to the Headteacher. Passwords should be changed regularly.

Software/hardware:

- School has legal ownership of all software and holds appropriate licenses. Equipment and software are regularly audited by the Headteacher in conjunction with schools ICT technician.

Managing the network and technical support:

- Technical support is provided by Rushtons Ltd

Filtering and virus protection:

6. Our Internet Filtering (Lightspeed Systems) service is a centrally hosted web filtering provision enabling safe internet access for schools.

7. Education and Training

Regular updates on Online Safety, curriculum resources are discussed in staff/team meetings.
Pupils are made aware of the risks associated with the use of technology through the curriculum.

6.1 Online Safety across the curriculum

Pupils are taught how to take a responsible approach to their own Online Safety through a range of curriculum areas.
Rosegrove Infant School use Hector's World online safety tool. This allows children to cover material which they are unsure of and the children are taught to let an adult know so it can be investigated.
A link to the following website is provided on both school and nursery's websites and provides resources and more information on this tool:

www.thinkuknow.co.uk

E-Safety is taught throughout the computing units of work and is supported by material from the Espresso online learning resource.
Recommended stories are also used to support children staying safe online.

6.2 Online Safety – Raising staff awareness

Online Safety training for all staff is available through learningzone.lancashire.

6.3 Online Safety – Raising parents/carers awareness

Parents/carers will be made aware of the benefits and risks associated with the use of technology through newsletters and via the website.

6.4 Online Safety – Raising Governors' awareness

Governors awareness of Online Safety issues will be discussed at Governors meetings.

7 Standards and inspection

The Online Safety policy will be monitored and reviewed by the Online Safety Champion/Headteacher on an annual basis. Risk Assessments on new technologies used in school will be carried out when needed. Incidents of misuse will be monitored and reviewed by the Online Safety Champion/Headteacher and addressed within the school's policy and practices. Acceptable Use Policies will be reviewed annually.

Signed	**Signed** **On behalf of the Governing Body**
Head Teachers name: **Mrs L Renshaw**	**Chair of Governors name;** **Mrs L Lingard**
Date:	**Proposed Review Date.**

Appendix

Information for Staff and Governors of Rosegrove Infant School

Lightspeed Systems – Internet Filtering (provided by BT)

What is it?

Our Internet Filtering (Lightspeed Systems) service is a centrally hosted web filtering provision enabling safe internet access for schools.

Why do I need it?

It provides you with the flexibility to locally manage and control access to websites. The service provides the following functionality for schools:

- Education focussed web filtering.
- Ability to filter based on IP address ranges or by using an external directory such as your School's active directory domain.
- Local control to allow your School to manage which websites it wishes to allow or block.

What are the benefits?

Schools have the ability to implement granular filtering based on individual classroom or user needs, removing dependence on BT Lancashire Services to block / unblock individual websites for individual school requests.

Schools do not require any filtering equipment to be installed in school with this service.

What's Included?

Service Features

Feature	Description
Internet Filtering	The centrally hosted and managed filtering service provides safe internet access for schools, managing all web traffic from BT Lancashire Services broadband connected schools (Cumbria schools will need to request access via our Service Desk).
Global Filtering (All schools – default setting)	BT Lancashire Services have initially assigned a default filtering set based on school type (Primary / Secondary), which should meet most schools' needs. Your School can then choose to tailor this to your individual requirements. The Global Blocked Categories are as follows (these cannot be overridden by schools in the local settings): • Drugs

	• Gambling • Offensive • Porn • Porn illicit • Violence • Security • Security nettools • Security proxies • Weapons
Local Control of Filtering (No filtering hardware required in school)	• Local control option is built in to give your School more flexibility to set filtering to suit your School. Your School has the ability to block or unblock individual websites. • Filtering can be based on IP address ranges or by using directory services such as active directory. • Certain websites, including illegal sites or categories of websites classed as inappropriate by the Lightspeed Filtering service, are blocked at a global level and cannot be amended, ensuring protection for pupils and staff. All other categories are available for your School to select as either allow or block. • This service may require your technical support staff to configure services locally. In view of the levels of flexibility offered with the Internet Filtering service, your School has full responsibility for managing access to websites and to ensure that staff, pupils and guests can **only** access appropriate content using either a School device or personal device on the network. • Support articles on using the filtering service and access to Lightspeed Systems Wiki are provided to ensure that you have advice on functionality. Full details are available on our filtering support pages on our website.

Service Support

Support	**Description**
Support features	Support provided: • Guidance materials for the setting of allowed / blocked sites • Guidance materials for the configuration of PCs / laptops / tablets • Guidance on submission of URLs to Lightspeed Systems, if a website is incorrectly categorised in the global settings • Global rocket administration settings (not individual school's administration) • Guidance materials for reporting • Guidance materials for override options
Support from BT Lancashire Services ICT Service Desk (please refer to exclusions)	Operational from 8am to 6pm (Monday – Friday excluding Bank Holidays and statutory leave days), with escalation routes ensuring that, if your school does experience problems with the service, our staff are focussed on solving your issues.

What Does it Cost?

Service	Annual Charges £ (Ex VAT)
Lightspeed Internet Filtering Service	Inclusive within the annual charge for your School's Broadband bundle.

Notes
We do not currently offer this service separately from our broadband packages.

What's Excluded?

- The current configuration of the filtering service does not include SSL/HTTPS packet inspection (this feature is currently being reviewed for implementation).

Your School will be responsible for the following when using the service:

- Ensuring that the correct IP range (as assigned by BT Lancashire Services with your broadband connection) is being used and to check for proxy issues.
- Setting of locally allowed / blocked sites.
- Configuration of PCs / laptops / tablets for web filtering.
- Bring incorrectly categorised sites to the attention of Lightspeed Systems via http://archive.Lightspeedsystems.com/resources/Databases.aspx
- Connection of devices to the internet / performance of devices.
- Referral of any third party web services authentication issues to your third party.
- Configuration of Lightspeed to the school's Active Directory (to enable year group filtering if required).