Rushen Primary School

e-Safety Policy

Approved by:		**Date:** September 2022
Next review due by:	September 2024	

Introduction

This policy is designed to run alongside the Department of Education, Sport and Culture's Acceptable Use Policy (AUP), Safer Schools App and Rushen Primary School's current ICT curriculum.
All children must be made aware of the AUP points and Inappropriate Content Protocol (IICP) every academic year.

The aims of this policy:

- To create consistency in the processes that protect children.
- To communicate expectations in the protection of children.
- To define the role of the e-safety policy in collaboration with other school policies that influence teaching and learning.
- To ensure that all members of our learning community understand the importance of staying safe in a digital world.

Online

Access to the internet:
Children should always be supervised when using ICT equipment to browse the internet. There should be no unsupervised use of ICT equipment during non-teaching time. For example, break and lunchtimes. Teachers will use a number of strategies to manage children using the internet in lessons including:

- providing a range of suitable websites.
- walking around and discussing with children the content they are viewing.
- If not all children on devices can be monitored then they should not be on internet ready equipment, group/paired learning may be more appropriate.

Staff will be proactive in monitoring what children are doing on the internet, they will discuss what they have viewed, highlight safer searching and image filters, look for minimised windows and tables. All staff will be aware of the Internet Inappropriate Content Protocol (IICP) (appendix 1) to follow if a child views something inappropriate on the internet.

Web filtering:
The department of education, sport and culture (DESC) have web filtering set up in school and this should block most inappropriate content, sometimes things do get through and the IICP (appendix 1) should be followed if a child views something inappropriate on the internet. Children should be aware of their role in reporting any inappropriate content to staff.

Use of pupil devices to bypass web filtering:
3G and 4G pupil devices are not presently routinely allowed into school.

Social networking sites:
The use of the Safer Schools app within KS2 in schools and at home supports Rushen Primary School's e-safety curriculum and stance on the use of social networking sites by our pupils. Whilst we do not encourage (and actively discourage) the underage use of social networking sites such as Facebook, Instagram, Tik Tok and Snapchat we will educate pupils in the dangers associated with social

networking sites as part of our e-safety curriculum. We aim to educate all stakeholders using the Safer Schools app and advice from DESC.

Appropriate behaviour (including cyberbullying):
Cyber bullying for children will be dealt with as per our Anti-bullying policy. Staff should model good practice in terms on their behaviour when using technology. There is an expectation that parents will model appropriate behaviours online.

Online Gaming:
Rushen Primary School will provide guidance to parents/carers via the Safer Schools app on the topic of online gaming and how to protect their children in this space.

Personal Data
All staff laptops are to be password protected and are encrypted to ensure content on them is secure.

School's storage and use of images:
The school uses the Department of Education, Sport and Culture's wording on its photograph/video disclaimer letter and this is sent out at the beginning of the child joining our school. A reminder to update permissions is sent out at the beginning of every school year. Records of children who may/may not be photographed/videoed are kept on Arbor and checked by class teachers regularly.

When taking photographs all staff should follow these guidelines:

- Personal devices (e.g. phones) should not be used for taking photographs of children. (If for any reason this is necessary (and agreed by SLT) then photos must be downloaded onto a secure space using a school device and must be deleted immediately from the staff members personal device.)
- Photos on devices should be removed periodically (at least once a year) when they are no longer required.
- Devices that contain photos of children should not be removed from school. Ensure any device containing photos is wiped before it leaves the school premises e.g. for a trip.

Staff should delete photographs of children who are no longer at the school unless the photographs are being kept as examples of particular educational practice or similar.
The use of pen drives for photographs by staff or children is not allowed. Photographs must only be stored on encrypted staff devices or the secure cloud server.

Holding sensitive data:
Sensitive data is any information stored that allows children or groups of children to be identified and may include: names (first and surnames), DOB, addresses, phone numbers, class lists, reports, child protection records, passwords, staff observations and performance management records, SEN register etc.
No sensitive data should be placed on pen drives, their use is not allowed in school.
It is the responsibility of all members of staff to ensure they have secure passwords set on files/programs which contain sensitive information.

Student use of personal information:

Children will be educated about personal information as part of the school's e-safety curriculum.

Passwords:
From Year 3 upwards children will change their passwords to more secure passwords and will be educated in how to create secure passwords as part of the school's e-safety curriculum. If a member of staff or a child feels their password is not secure or that someone else knows their password they should change it straight away.

Curriculum

Education and training for students and parents:
The school's e-safety curriculum is designed in accordance with the Safer Schools app and to raise awareness/give children the knowledge and understanding they need to be safer online, reducing the risk. The curriculum is progressive from Reception to Year 6. Differentiation of access to the curriculum and differentiation of the curriculum will be considered by teachers with consideration of vulnerable groups (very internet savvy, SEN needs and difference in disgust levels/home background). The curriculum has been designed to appeal to and cater for a range of differing learning styles. The school's e-safety curriculum will be flexible to reflect and meet the learning needs of the children in each class and the continuous development of technology.

Deliver:
The e-safety curriculum will be inherent in ICT and curriculum teaching and learning, will feature in assemblies and will be taught as a focussed unit throughout the year. The school will highlight related events such as Safer Internet Day which will be used to heighten awareness.
The school will advertise and advise how to use the Safer Schools app to families periodically and a proactive approach will be taken wherever possible.

Sanctions for misuse

Confiscating personal items:
Personal devices are not needed in school and will be confiscated. Any child who needs to bring in a personal device is advised to leave it in the office and collect it at the end of the day. Laptop/iPad privileges may be removed in line with IICP (appendix 1).

Clarity over accidental, deliberate or illegal access to inappropriate material:
See IICP (appendix 1) for this. This should be reported to a member of SLT to be recorded in the Internet incident log.

Sanctions for bullying, harassment, sexual exploitation, racial or hate motived incidents:
Will be in line with the school's anti-bullying and behaviour policies.

Staff responsibilities

Modelling good practice:
Staff will make parts of their everyday practice explicit to the children to reinforce good e-safety practice. For example, deleting photos, using safe search filters for images, having a screen saver set and entering a password.

As part of following teaching standards, all staff will follow the school curriculum for ICT when planning lessons.

Adhering to policies and knowing when to escalate e-safety issues:
All staff will be aware of and follow the DESC AUP. They will also familiarise themselves with the IICP (appendix 1) and other parts of related policies (anti-bullying/behaviour). A log of internet incidents will be kept by the SLT and kept in the Headteacher's office.

Maintain a professional level of conduct in their personal use of technology both within and outside:
See point 6 on the AUP as this has clear instructions for staff.

Take personal responsibility for their professional development in this area:
It is the responsibility of staff to highlight and address their own training needs in relation to ICT and e-safety. The ICT co-ordinator, department and other staff will aim to provide training as appropriate.

Reviewing policy

This policy will be reviewed on a 3 year basis or as the need arises and will be highlighted to all staff at the start of each year. The policy will be highlighted to new teaching staff as part of the schools induction policy.

Appendix 1

Internet Inappropriate Content Protocol

This policy outlines steps to be taken to prevent children from viewing inappropriate content on the internet and also outlines steps to be taken should this situation arise. The policy is taken from the Department of Education, Sport and Culture's guidance for Internet Safety.

Children must be supervised at all times when using the internet and what they are viewing should be monitored.
This applies in all lessons and during any lunchtime or after school clubs. This supervision may be by talking to the children about what they are doing, viewing their screen during walk around.

Steps to follow in the event of child/children viewing inappropriate content on the internet:

If you notice a child viewing something unsuitable or a child reports that they have seen something unsuitable do **NOT** quit the browser, instead simply click the back button or minimise.
Talk to the children about what they have seen, what they were searching for and who saw

it?
If there were others around who viewed/saw the content get their names too.

It may also be useful to view the History to see what else the children have been looking at. Copy the URL (website address) into an e-mail and send this to GTS who will block the site.

Speak to a member of Senior Leadership Team and explain what happened and the circumstances.

The Head/Deputy head will advise what action is to be taken:

This may be to phone the parents to explain that their child has accessed an unsuitable site/image and your understanding of why/how (by accident, innocent or searching on purpose etc)
It should be pointed out to parents that schools have very effective internet filtering called but that sometimes it is still possible to find unsuitable material. Parents may wish to know the nature of the viewing so that they can discuss/follow up this at home with their child.

A log of instances where children have viewed inappropriate content/images on the internet will be kept and all occurrences should be logged by a member of the Senior Leadership Team and the member of staff supervising the children at the time.