**Online Safety in Cardross Primary School**

**(Updated) March 2020**

**I**[**ntroduction**](#_heading=h.1fob9te) **2**

**Managing Internet Access 2**

Information System Security 2

E-mail 2

Published Content and school website 2

Publishing work 3

Social Networking and personal publishing 3

Managing filtering 3

Managing emerging technologies 3

Other devices 3

**Protecting personal data 4**

**Policy decisions 4**

Authorising internet access 4

Assessing risks 4

Handling eSafety complaints 4

Community use of the internet 4

**Communications Policy 4**

Introducing the eSafety policy to pupils 4

Staff and the eSafety policy 5

Parental support 5

**Appendix : 6**

Appendix 1 Remote Learning

Appendix 2 Argyll and Bute Social Media Policy Link

# Introduction

# At Cardross Primary:

* Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use
* Pupils will be educated in the effective use of the Internet
* Pupils will be shown how to publish and present information appropriately to a wider audience
* Pupils will be taught how to evaluate Internet content
* The school will seek to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law
* Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy
* Pupils will be taught how to report unpleasant Internet content e.g. using the CEOP Report Abuse icon.

# Managing Internet Access

# Information system security

* School ICT systems security will be reviewed regularly
* Virus protection will be updated regularly
* Security strategies will be discussed with the IT provider

# E-mail

* Staff may only use approved e-mail accounts on the council’s corporate system and GLOW accounts set up by the administrator while in school
* When staff email communication occurs, it must only take place via a school email address or from within the school learning platform
* Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known
* Pupils will be taught not to reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission, and of the dangers associated with such behaviour. Pupils will not be provided with a GLOW or school email account at this time

# Published content and the school web site

* The contact details on the Web site should be the school address, e- mail and telephone number. Staff or pupils personal information will not be published
* The Head teacher and the Website coordinators (SLT) will take overall editorial responsibility and ensure that content is accurate and appropriate

# Publishing photographs, images and work

* Written permission from parents/carers will be obtained for the taking and publishing of photographs or video
* Photographs that include pupils will be selected carefully and full names will be not be used on the Web site or learning platform, as appropriate, including in blogs, forums or wikis, particularly in association with photographs
* Parents will be clearly informed of the school policy on image taking and publishing, both on school and independent electronic sources

# Social networking and personal publishing on the school learning platform

* Pupils will not have access to social networking sites at school, but the school will educate pupils in their safe use e.g. use of passwords
* They will be advised never to give out personal details of any kind which may identify them, anybody else or their location
* Pupils must not place personal photos on any social network space provided in the school learning platform without permission
* Pupils, parents and staff will be advised on the safe use of social network spaces
* Pupils will be advised to use nicknames and avatars when using social networking sites

# Managing filtering

* The school will continue to work in partnership with Argyll and Bute eSafety team (Child Protection and Education) to ensure systems to protect pupils are reviewed and improved
* If staff or pupils come across unsuitable on-line materials, the site must be reported to the nominated member of staff
* The school will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable

# Managing emerging technologies

* Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed

# Other devices

* Mobile phones and associated cameras will not be used during lessons or formal school time except as part of an educational activity
* The sending of abusive, offensive or inappropriate material is forbidden (See Anti-bullying policy)
* Games machines including the Wii, Sony Playstation, Microsoft Xbox and others that have Internet access cannot join the school network so must be played offline. Care will be taken with their use within the school

# Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

All members of staff will undertake GDPR training and must update this annually

# Policy Decisions

# Authorising Internet access

* All staff must adhere to the Argyll and Bute Council Acceptable Use Policy when using ICT
* Parents will be asked to sign and return consent forms within annual Permissions return
* Pupils must agree to comply with the Responsible Internet Use statement before being granted Internet access

# Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Argyll and Bute Council can accept liability for the material accessed, or any consequences of Internet access.

# Handling eSafety complaints

* Complaints of Internet misuse will be dealt with by a member of the senior leadership team
* Any complaint about staff misuse must be referred to the Headteacher and a E-Safety Concern form completed
* Complaints of a child protection nature must be referred to the Headteacher and dealt with in accordance with school child protection procedures
* Pupils and parents will be informed of the complaints procedure
* Pupils and parents will be informed of consequences for pupils misusing the Internet

# Communications Policy

# Introducing the eSafety policy to pupils

* Appropriate elements of the eSafety policy will be shared with pupils
* eSafety rules will be posted in all classrooms
* Pupils will be informed that network and Internet use will be monitored
* Curriculum opportunities to gain awareness of eSafety issues and how best to deal with them will be provided for pupils

# Staff and the eSafety policy

* All staff will be given the School eSafety Policy and its importance explained
* Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential
* Staff should not use school laptops to access wireless networks outwith Cardross Primary. Anyone wishing to do so must complete a VPN request to be submitted to the Head of Service for approval
* Staff who manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues

# Enlisting parents’ support

* Parents and carers attention will be drawn to the School eSafety Policy in newsletters, the school handbook and on the school website
* Parents and carers will from time to time be provided with additional information on eSafety through workshops and Family Learning events
* The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school

**Appendix One**

**Remote Learning**

There are a number of options we may consider to continue engaging with our learners during emergency school closure and to ensure we continue to support our pupils’ learning and health and wellbeing. This may include uploading of home learning tasks, providing access to online resources, and instructional videos. To help safeguard staff and children we have to consider the following:

|  |  |  |
| --- | --- | --- |
| Organisation | Participation | Technology |
| Do school online safety policies (Acceptable Use/Safeguarding/Standards reference online teaching) | What are the expectations of participation? | Do staff and children have the necessary technology and access? |
| How will Safeguarding be managed and have staff been trained? | What work will pupils be asked to do and when? | Who will provide technical support to staff, pupils and parents? |
|  |  | Have the technology service terms and privacy statements been considered? |

**Policy**

* Staff to familiarise themselves with the school online policy and what this means for remote learning.
* Remind all staff and students of Acceptable Use – this will still apply during school closure
* School will provide regular eSafety information to parents on Twitter and Seesaw - Wake Up Wednesday material from [www.nationalonlinesafety.com](http://www.nationalonlinesafety.com)
* Avoid one to one online tuition to help safeguard children and staff.

**Learning Platforms**

* We will use Seesaw and GLOW – Google Classroom for remote learning.
* Teachers will post activities and students will post responses. Parents can see all of their child’s work and can comment on it online.

**Safeguarding**

* Online or offline, effective safeguarding requires a whole school approach. Planning for remote learning activities should include safeguarding policy.
* Remind staff of safeguarding obligations. Report any safeguarding concerns according to school policy.
* Remind pupils of who they can contact within the school for help or support.

**Appendix Two**

Argyll and Bute Social Media Policy November 2014 Version 2.1