Scoill yn Jubilee E-safety Policy

Scoill Yn Jubilee

E-safety Policy 2013

1. Online

1.1 Access to the internet is available to all staff and children through laptops, desktops and iOS devices. The internet is filtered through a DEC controlled filter, however it cannot filter out all inappropriate materials. Access to social networking sites, external email and YouTube is restricted to staff only through a secure login.

1.2 Children will only access the internet when a teacher is present. All internet access at school should be supervised. Supervision means more than being in the room, a teacher needs to be actively involved in what the children are doing. Teachers should engage the students in conversation about what they've found out and should promote responsibility and trust. If necessary teachers should conduct random checks on devices, including the history and browser windows. Following an incident random checks will take place until teachers judge children as being able to act in a responsible manner.

1.3. Children should be made aware of the rules for appropriate internet use and the consequences if not used correctly. Parents must acknowledge they have read the AUA with their at the start of each academic year. Children must abide by the school rules on acceptable behaviour online. Cyber bullying is not accepted. Any incidents of cyberbullying will be fully investigated and when necessary outside agencies, including the police, will be involved. All incidents of bullying will be treated in accordance with our behaviour and bullying policy.

2. Personal Data

2.1 All data needs to be secure, including images. Images on a camera should be uploaded onto a computer then deleted. If teachers personal cameras are used then images must be deleted within 24hrs. Pen drives can be made secure by encrypting but SD cards on cameras cannot. When taking photographs in the classroom and around the school staff need to make sure there are no notices, class lists or details of children in the background. Images should not be stored on laptops longer than necessary. Where possible, all images should be stored on the ‘cloud’ and consideration should be given to deleting images after one year.

2.2 Images taken are for school use only. Images taken of children may be used on the school’s private pupil wiki. Select images may be used on the school’s public blog. Names of children must not be published on the public wiki and blog. First names only may be used on the private pupil wiki.

2.3 Staff laptops must have automatic screen lock turned on - to come on in less than 7 minutes. Access to IMPs must be password protected, if for any reason a password is no longer requested, the staff member must inform ICT Helpdesk and ask for it to be returned to password protected.

3. Embedding e-safety across the curriculum

3.1 E-safety curriculum needs to be referred to frequently as an integral part of learning. Each class teacher will be responsible for teaching and regularly monitoring the children's use of ICT in their classroom. e-safety and acceptable use of ICT must be reinforced and embedded throughout all year groups and Key Stages. At the beginning of each year every class will create a list of e-safety rules to refer to throughout the year. Teachers should make use of online material provided by the Isle of Man DEC to support eSafety (https://www2.sch.im/groups/esafety/)

4. Involving students and parents

4.1 Parents will be offered support and guidance about e-safety through sharing of information on the school wiki, e-safety leaflets and e-safety presentations.

4.2 The school will become involved in events such as E-Safety day and other initiatives which promote the safe use of the internet. It will actively seek the views of parents and the wider community and encourage parents to liaise if they think a student is either at risk or showing inappropriate behaviour online.

5. Personal Devices

5.1 Children must not bring in personal electronic devices. If mobile phones are needed for after school use, they must be submitted to the school office. A consent form should be signed by parents to allow children to bring in a mobile phone.

5.2 If for special projects personal electronic devices are allowed to be used in class, parents will be formally informed if children are allowed to bring in a device and a permission slip will be sent out on each occasion. Children and parents must have acknowledged the school's Acceptable Use Policy before bringing any device into school.

5.3 Devices brought in from home with 3G can bypass school filtering systems and present a new route to undesirable material and communications. Care is required in any use in school or other officially sanctioned location. Children should use the schools wifi 'DECGuest' network, that filters searches when accessing the internet.

5.4 If children bring in a personal device without permission it will be confiscated and parents will be informed. Children will have to collect their device at the end of the school day.

6. Responding to Issues and sanctions for misuse

6.1 If members of staff suspect that misuse might have taken place, it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.
It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures . The school will keep a record of incidents that occur in the e-safety incident log book.

6.2 The table below shows possible disciplinary procedures that may be followed

	refer to class teacher	Record in e-safety incident book	Refer to Head teacher/ Deputy Head teacher	Head to Report incident to Police	Temporary removal of internet access	Inform parents
Deliberately accessing or trying to access material that could be considered illegal	✓	✓	✓	✓	✓	✓
Unauthorised use of non-educational sites during lessons	✓				✓	
Unauthorised use of mobile phone / digital camera / other handheld device	✓	✓	✓			✓
Unauthorised use of social networking / instant messaging / personal email	✓	✓				
Unauthorised downloading or uploading of files	✓	✓				
Allowing others to access school wiki/Google Docs by sharing username and passwords	✓	✓	✓			✓
Attempting to access the school wiki/Google Docs, using another pupil's account	✓	✓	✓			✓
Corrupting or destroying the data of other users	✓	✓	✓		✓	✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓			✓
Continued infringements of the above, following previous warnings or sanctions	✓	✓	✓	✓	✓	✓
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✓	✓	✓		✓	✓
Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓	✓			✓
Deliberately accessing or trying to access offensive or pornographic material	✓	✓	✓	✓	✓	✓
Deliberately distributing offensive or pornographic material	✓	✓	✓	✓	✓	✓

7. Staff responsibilities

7.1 All staff are responsible for modelling good practise and adhering to school policies regarding e-safety. Staff set an example in terms of e-safety by having secure passwords, using mobile devices in an appropriate way during learning time (e.g not texting, social networking, personal use etc), talking through appropriate use of social networking.

7.2 Staff must maintain a professional level of conduct in their personal use of technology both within and outside of school. Staff must not bring the DEC or school into disrepute with social networking and FirstClass emails, and act within the DEC AUP and whistle-blowing policy.

7.3 Staff are encouraged to take personal responsibility for their professional development e-safety by use of Isle of Man DEC wiki and other online material. All

staff will engage with professional discussion at staff meetings/twilights/ professional forums and will seek appropriate support where needed.

7.4 It the responsibility of staff to know how and when to escalate e-safety issues - staff to decide if the issue is aggravated, intentional or accidental and follow the eSafety sanction table referred to in section 5 of the eSafety policy.

8. Vulnerable groups

8.1 The school has a duty to safeguard and promote all children's welfare in relation to children's understanding of e-safety issues. We interpret this duty to include a child's e-safety in their home, and will work with parents and external agencies (where appropriate) to promote safe and appropriate use of children's online access, gaming access, social networking and use of mobile devices.

9. Reviewing Policy and evaluating effectiveness

9.1 The e-safety and AUA policies will be implemented through curriculum development meetings and will be monitored through discussion and use of e-safety incident log. The school will provide training and support to enable staff, pupils and parents to understand the school's policies and the importance of e-safety in schools and at home. The policies will be revised and revisited each year or when appropriate to reflect changing technologies and new initiatives.

9.2 Pupils will be included in developing and reviewing our e-safety and AUA policies. When appropriate the school will encourage active learning methods including posters, promotional videos leaflets and class assemblies. Policies can be accessed via the school's wiki. Parents will be informed about updates and information in school newsletters.

9.3 In order to evaluate the effectiveness of our policy the school will use a range of strategies including staff/pupil interviews and audits, monitoring pupil behaviours whilst using technology in school and evaluating the communication received from both children and parents.

Monitoring, Evaluation and Review

This policy will be reviewed on a three year basis or when the need arises, to assess its implementation and effectiveness. The policy will be promoted and implemented throughout the school.

Governor Approved February 2014
Review February 2017.