Scoill Phurt le Moirrey

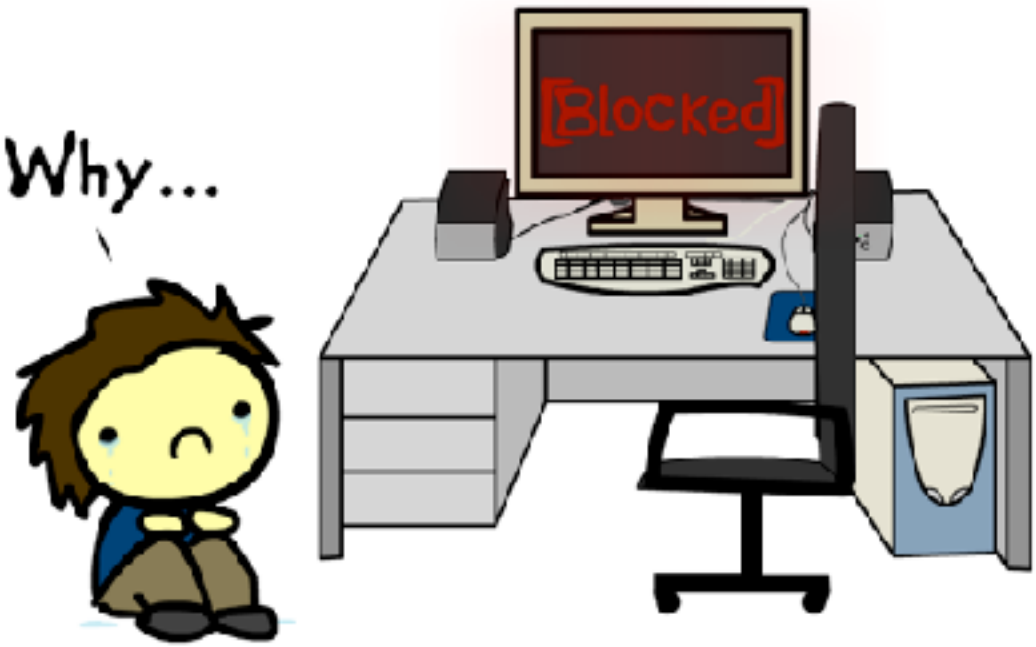
E-safety Policy

This policy reflects the views and discussions of teaching staff at Scoill Phurt le Moirrey and is designed to run alongside the schools 'Acceptable Use Policy' (AUP) and 'Internet Inappropriate Content Protocol' (IICP), that have been influenced by the Department of Education and Children's own user agreement.

The aims of this policy:

- To create consistency in the processes that protect children.
- To communicate expectations in the protection of children.
- To provide references for the documentation required to protect children.
- To define the role of e-safety policy in collaboration with other school policies that influence teaching and learning.
- To raise the progress and attainment of learning across the whole school.
- To ensure that all members of our learning community understand the importance of staying safe in a digital world.

All children must be made aware of the 12 points contained within the AUP at least once a year. The school's ICT curriculum, and the dedicated e-safety section within, reinforce the statements made in this policy.



Accessing 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. Teachers will use 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 laptops 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 safe searching and image filtering that supports the search as implemented by the Department of Education and Children (see below). Staff will be able to look for minimised windows and tabs. All are expected subject matter for teaching from the school curriculum. All staff will be aware of the 'Internet Inappropriate Content Protocol' (IICP) to follow if a child views something inappropriate on the internet.

Web filtering

The department of Education and Children ICT department have web filtering applied in school to all devices and this should block most inappropriate content. The nature of the technology and the size of the challenge means that sometimes content will get through and the IICP 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 and staff should be conscious of the different levels of disgust and fear amongst all of the school's children.

Use of alternative networks

3/4G Devices that enter the school's site for the use of children should be configured to use the school's guest network (DECGuest, password: 'sp3lling'). This is to override the ability of the device to bypass the content filters of the school network. Staff should be mindful of using personal devices that may be configured to access 3/4G networks when working with children to manage avoidable accidents, including the displaying of inappropriate material when linked to a projector or otherwise.

Management and use of the school website

It is agreed that whole school events will be posted on the school website as well as anything that staff feel is newsworthy. This maybe whole school or class based. This website is to publicise and promote our school. Lesson and learning related content is can also use alternative online spaces including Googledocs and/or itslearning where a learning dialogue can be established with the children.

It is agreed that staff will correct typing and visual mistakes they spot where capable on the school website, however content changes will be discussed with the author of that page before doing so. If they are unable to make the change then they will notify a member of staff who can do so. Moderation of any communication using social networking plugins, including Twitter (see social networking sites), will be the responsibility of the school Senior Leadership Team. The use of an alias name or nickname will be promoted for children who may comment on the content of the school website.

Social networking sites

Scoill Phurt le Moirrey has a clear stance on the use of Social Networking Sites by its students and this is explained in our 'Internet Safety leaflet'. Whilst we do not encourage (and actively discourage) the underage use of social networking sites such as Facebook, Snapchat and Twitter, we will respond to the demands of societal use by educating in how to make these accounts more secure. We will also make pupils aware of the dangers associated with such social networking sites, both aspects being part of our e-safety curriculum. We aim to educate parents by sending literature home that encourages an open dialogue regarding the issues around the subject.

Appropriate behaviour (including cyberbullying)

Cyber bullying will be dealt with as per our Anti-bullying policy.

Staff should model good practice (aided by our curriculum) and in terms of their behaviour when using technology. Staff will adhere to the 'DoEC's Guidelines on the use of Electronic Communications and Social Media (2015) when using such sites on personal as well as Department devices.

The Management of Data

The Security of Data

All staff laptops are password protected and are encrypted to ensure content on them is secure by Government Technical Services (GTS). This system requires all members of staff to reset their password every 42 days and is inclusive of parameters when doing so e.g. use of a capital letter.

Pupil laptops are secured by the DoEC's network security system to prevent access from external attacks.

School's storage and use of images

The school uses the Department of Education and Children's wording on its photograph/video disclaimer letter and this is sent out at the beginning of each year. Records of children who may/may not be photographed/ videoed are kept by the school office.

When using cameras, iPads or other devices capable of recording photographs and video (visual data), all staff should follow these guidelines:

1. Ensure the memory of the device is wiped before use.
2. Download the visual data taken on the same day.
3. Delete the visual data once downloaded from the device.

Devices should not be removed from the school that have recorded visual information containing children.

Staff should delete visual data of children who are no longer at the school unless the information is being kept as an example of particular educational practice or similar. This includes visual data on personal devices that should only be used as a last resort to record an event in the first place.

The use of pen drives to store or move any data, visual or otherwise, containing staff or children is not allowed when using any device that is supplied by the Department of Education and Children. This includes visitors to the school.

Holding sensitive data

Sensitive data is any information stored that allows children, groups of children, staff or groups of staff to be identified and may include: names (first and surnames), DOB, addresses, phone numbers, class lists, reports,

Child protection records, passwords, staff observations & performance management records, SEN register etc.

No sensitive data should be placed on online storage or within communication services e.g. Googledocs or itslearning, that do not have a high enough level of encryption and protection. Such levels are dictated by the Isle of Man Governments e-safety policy and relate to European standards of data management.

It is the responsibility of all members of staff to ensure they have secure passwords set on files/programs which contain sensitive information e.g. ARBOR, pdf files etc. and that they are updated as and when necessary. This is to prevent unwanted access by others, physically or remotely. Passwords should not be recorded in written form, including digitally on a device (unless security is ensured by a password or alternate form of digital security) and should never be stored with a DoEC device.

When destroying any data for protection purposes, as you would shred paper copies, consideration should be made to emptying trash to ensure deletion.

Students use of personal information

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

Passwords

From Year 4 upwards children will be encouraged to 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 via the ICT Coordinator of the school. Staff can keep a secure record of all passwords for the children in their class on the Department of Education and Children's server (the cloud), which will be accessible by any member of staff that may be teaching that child at any time.

Curriculum

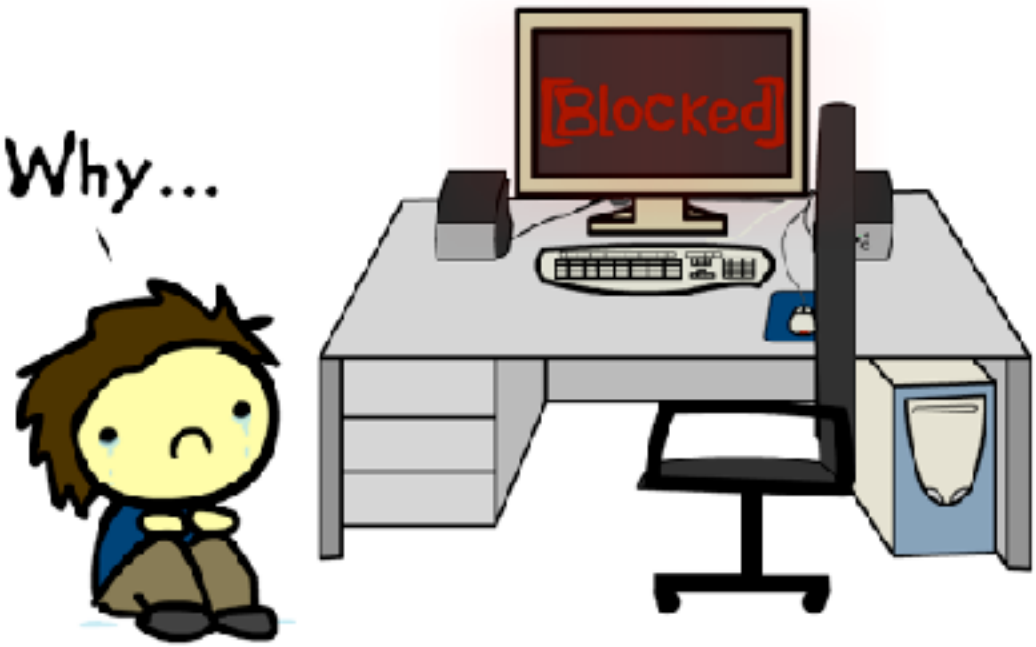
Education and training for students and Parents

The school's e-safety curriculum is designed to raise awareness and give children the knowledge and understanding they need to be safer online, reducing 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/fear levels and 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.

Delivery mechanism

The e-safety curriculum will be inherent in ICT & curriculum teaching and learning, will feature in assemblies and will be taught as a focussed unit during the year.

The school has a leaflet for parents. A proactive approach will be taken wherever possible.



Use of mobile devices (including mobile phones)

Mobile devices are allowed onto the school premises, but the school user agreement is immediately affective as signed by all pupils and observed by all parents each year.

If a pupil wishes to bring a personal device onto school premises for communication purposes at either end of the school day, or for learning, the first instance would see the device handed to the class teacher at the beginning of the day for safe and secure keeping within a locked container. In the second instance the following paragraph should be adhered to.

If a teacher wishes to allow personal devices into school for a specific learning experience (e.g. trip) they should liaise with the ICT Coordinator/ SLT as appropriate and provide an explanation as to how this would affect learning in a positive manner. This should be supported by a reminder of the user agreement that all pupils will have been asked to adhere to, and all devices must be connected to the school guest network to disable any satellite network access. Thus preventing the DoEC's filters from becoming inactive.

Sexting

If a device on school property has an explicit image of a pupil available to view on it, do not look at the image. Ask the person who has made you aware of it to describe it to you. If you are required to look at it then do so with at least one other person. Ideally the head teacher or safeguarding officer. Don't print it or email it to yourself, isolate it and attempt to get it removed from the internet

Sanctions for Misuse

Confiscation of items

Personal devices will be confiscated if the user agreement is not adhered to, and must be collected from the school by a parent or carer. Laptop privileges may be removed in line with **IICP** and the school behaviour policy will be enacted.

Accidental, deliberate or illegal access to inappropriate material

See the IICP. Such incidents should be reported to the ICT coordinator.

Sanctions for bullying, harassment, sexual exploitation, racial or hate motivated incidents

This will enact the school's anti-bullying and behaviour policies.

Staff Responsibilities

Modeling good practice

Staff will make parts of their everyday practice explicit to the children to reinforce good e-safety practice in line with the school ICT curriculum. e.g. 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, the unit concerning the teaching of e-safety contained within.

Adhering to policies & knowing when to escalate e-safety issues

All staff will be aware of and follow the school's AUP as influenced by the DoEC's AUP. They will also familiarise themselves with the IICP and other parts of related policies e.g. anti-bullying/behaviour that are required to carry out the protocol.

Maintain a professional level of conduct in their personal use of technology both within and outside school.

All staff will sign the DoEC's AUP agreement as part of maintaining a professional level of conduct when using technology in the school. This includes the acceptable maintenance of hardware for learning in the classroom.

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 coordinator, department and other staff will aim to provide training as appropriate.

Reviewing this Policy

This policy will be reviewed regularly due to the the rapidly changing nature of the subject matter, 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 procedures.

Monitoring Procedures & Evaluating effectiveness

The following are examples of strategies that will allow the school to monitor and evaluate the effectiveness of this policy.

- Pupil Interviews
- Staff discussions
- Pupil questionnaire
- Observed behaviours when using ICT equipment

All parents will be encouraged to have dialogue with the school regarding this policy so that the views of everyone in the community are instrumental in ensuring the effectiveness of this policy going forward. They will be encouraged to approach the school for support in the event of their child being at risk whilst online via literature in paper and digital formats.