Scremerston First School

Acceptable Use Policy

Reviewed September 2018- E.Holleywell

Scremerston First School AUP

Introduction

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Apps
- Email, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices including tablets and gaming devices
- Online Games
- Learning Platforms and Virtual Learning Environments
- Blogs and WikisPodcasting
- Video sharing
- Downloading
- On demand TV and video, movies and radio / Smart TVs

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements (13 years in most cases).

At Scremerston First School, we understand the responsibility to educate our pupils on e-Safety Issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and others to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for your school to use technology to benefit learners. Everybody in the school community has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, governors, regular visitors [for regulated activities] and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, SMART watches and other mobile devices).

Monitoring all internet activity is logged by the school's internet provider (The Lightspeed Rocket via Northumberland County Council.) These logs may be monitored by that provider as well as the Headteacher and e-safety coordinatior. A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual. For staff any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure or, for Support Staff, in their Probationary Period as stated. Policy breaches may also lead to criminal or civil proceedings. The Information Commissioner's powers to issue monetary penalties came into force on 6 April 2010, allowing the Information Commissioner's office to serve notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act. Incident Reporting Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's relevant responsible person. Additionally, all security breaches, lost/stolen equipment or data (including remote access/PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the relevant responsible person.

Computer Viruses

- All files downloaded from the Internet, received via email or on removable media such as a memory stick must be checked for any viruses using school provided anti-virus software before being used. **NB: All antivirus software utilises real-time protection and automatically scans & checks files/documents on removable media such as USB sticks before they are opened and read/edited. To manually scan all files on a USB stick before opening them, either in or out of school, right click on the USB stick icon in My Computer and select scan option using the respective antivirus software installed on the machine.**

- Never interfere with any anti-virus software installed on school ICT equipment.

- If your machine is not routinely connected to the school network, you must make provision for regular virus updates through David Harrison (ICT Technician).

- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know.

ICT Acceptable Use Policy: Staff and Pupils

Introduction

The internet is a valuable resource that can raise educational standards by offering both pupils and teachers opportunities to search for information from a very wide range of sources based throughout the world. However, some of the information to be found on the internet will be inappropriate for pupils and we feel it is important to have a policy in place that takes this issue into account. The school has a duty to ensure that before using the internet with pupils, staff have had the opportunity to discuss how they will deal sensitively with inappropriate use. The following policy helps to define appropriate and acceptable use by both staff and pupils and has been further discussed with Governors and pupils themselves. Please also refer to our Safeguarding and Child Protection Policy and Guidance for Safer Working Practice for Adults who work with Children and Young People in Education Settings. The implementation of this policy is the responsibility of all members of staff.

The Internet in School

The internet is a powerful technology, and we realise that it must play an important role in any learning environment. Through the internet, teachers are able to find information on topics they may be teaching, worksheets that have been written by other teachers and newsgroups of a particular interest to the school, and they will be able to share ideas with teachers around the region, nationally and internationally too. It aids planning and collaboration between schools. It provides an e-mail address to members of staff to enable them to keep in ready contact with other schools. Parents can contact staff members via the school email address.

The Internet in the Curriculum

The use of the Internet in the curriculum needs careful planning, and it should not be assumed that the children have the skills and knowledge of how to work safely in an online environment – for example, how to use search engines safely or to question the validity of sources. Therefore, if the internet is to be used, the teacher should ensure that these points are covered in the interests of accessibility, and also of safety.

School Website

Scremerston First School has a website and there are photographs which contain images of the children included in the content. Children in photographs are not be identifiable by name (ie. there will not be any captions containing the children’s names alongside photographs). If a child’s name is mentioned elsewhere (for example, because of some work that is displayed on the website), only the first name will be used and it will not be linked to any photograph of the child or any other personal details. The school does not publish personal email addresses of pupils or staff on the school website.

Roles and responsibilities

E-safety is recognised as an essential aspect of strategic leadership in this school and the Headteacher, with the support of Governors, aims to embed safe practices into the culture of the school. The Headteacher ensures that the policy is implemented and compliance with the policy monitored. Miss E.Holleywell is the e-safety lead and has completed online training. All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-safety procedures. Central to this is fostering a ‘No Blame’ culture so pupils feel able to report any bullying, abuse or inappropriate materials.

As the children progress through the school there is a gradual progression in access to the internet. Pupils will be made aware of unacceptable use of the internet without teachers being too explicit (as this may encourage some children to disobey the rules). The rules for using the internet will be made clear to all pupils and children will have to sign the Rules for Responsible Internet Use (see appendix) prior to using the internet. They will be made aware that if they feel that the rules do not apply to them and therefore decline to sign the agreement, then this will result in an instant loss of access to the internet. The rules apply to staff as well as pupils and staff (including temporary and regular supply teachers) will be asked to sign the Acceptable Use of the Internet form annually.

Monitoring

It is the role of both the Headteacher, Mrs Sarah Smith, and e-safety coordinator, Miss Emma Holleywell to monitor and evaluate the overall effectiveness of internet use throughout the school and they will do this on a regular basis. Each teacher will be responsible for monitoring the use of the internet within their classroom and ensure that unacceptable material is not accessed.

The Headteacher has responsibility for checking that no inappropriate material is on the school system and the children are made aware that teachers are able to view the content and duration of their internet usage.

David Harrison (The ICT Technician) ensures that the computer system is regularly checked for computer viruses with the SOPHOS system, taking advice from the school’s provider of technical support. School Windows platform equipment such as laptops/netbooks are real-time protected with either Sophos, Microsoft Security or AVG antivirus software all of which are allowed by LEA technical support. Full system scans of equipment are set by default and run in the background at regular intervals. Manual scans can be invoked by the ICT Technician when needed depending on equipment availability. School iPads do not require antivirus software as the Apple operating system is very robust against malicious code and overall faces fewer threats than Windows.

Managing the school network

Scremerston First School uses the “Small School Server” which is provided through county (Alan Smith) and is made available to pupils to further their education and to staff to enhance their professional activities including teaching, research, administration and management.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet or email activity on the network, or perform any other activities that the school may see fit.

All school laptops issued to teachers are monitored by “Future Cloud.” This means that any content viewed on these devices that may be inappropriate in nature can be captured automatically and viewed by NCC, E.Holleywell and S.Smith.

Personal Use

The computers, electronic media and services provided by the school are primarily for educational use to assist staff in the performance of their job. Limited or incidental use of electronic media for personal purposes is acceptable, and all such use should be done in a manner that does not negatively affect the system’s use for their educational purposes. However, staff are expected to demonstrate a sense of responsibility and not abuse this privilege. No personal devices should access the school’s wireless internet without permission from the Headteacher. Scremerston First School expects any staff using social media sites to ensure that their use is conducive to their professional status. They should not mention the school by name or in passing including on personal profiles, or discuss individuals or groups within the school, or compromise the school values. In addition, staff must ensure that any private blogs, bulletin boards, websites etc. which they create, or actively contribute to, do not compromise, and are not confused with, their professional role. Staff must ensure that any engagement in any online activities does not compromise their professional responsibilities.

Scremerston First School Rules for Responsible Internet Use by Pupils

The school has purchased iPads, netbooks and Internet access to help our learning. These rules will keep everyone safe and help us to be fair to others.