Acceptable Use Policy

DETAILS OF POLICY	
Original policy created by:	Jo Sedgwick
Date of most recent review:	October 2018
Reason for review:	Update
Adopted by:	SLT
Parties communicated to:	All stakeholders
Methods of Communication:	School intranet, induction
Next planned review date:	October 2020
Persons responsible for audit review of policy:	Whole staff group

Acceptable Use Policy

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 • E-mail, Instant Messaging and chat rooms • Social Media, including Facebook and Twitter • Mobile/ Smart phones with text, video and/ or web functionality • Other mobile devices with web functionality • Gaming, especially online • Learning Platforms and Virtual Learning Environments • Blogs and Wikis • Podcasting • Video Broadcasting • Music Downloading

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly webbased 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, usually 13 years.

At SwitchED2 we understand the responsibility to educate our pupils on eSafety 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 other people 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 the school to use technology to benefit learners.

Everybody in the school 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 are made aware of the risks and threats and how to minimise them.

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

The Aims of the Acceptable Use Policy are to:-

Allow all users access to school ICT resources and use of the Internet for educational purposes. Provide a mechanism by which staff and pupils are protected from Internet sites, information, and individuals that would undermine the principles and aims of the school. Provide rules which are consistent, and in agreement with the Data Protection Act 1984, Computer Misuse Act 1990 and other legislation relevant to the use of computers and electronic data in schools. Provide rules that

are consistent with the acceptable procedures commonly used on the Internet, including those associated with netiquette. Provide rules relating to the use of computers and ICT facilities in school, which are consistent with the general policies of the school.

General Internet use and Consent Pupils who are to have access to the internet must understand the basic conventions and navigation techniques before going online and accessing material. Pupils must have returned a signed consent form before being allowed to use the ICT facilities that involve accessing the internet. The use of the names of pupils or photographs of pupils for websites will require written permission from parent(s)/guardian(s) included on the use of photos consent form. If a picture is placed on the website the child's full name will not be displayed.

Pupils must not use the school ICT facilities without the supervision of a member of staff. Although use of the ICT facilities and access to the Internet will be supervised, and all possible measures will be taken (including the use of filtering and firewall), SwitchED2 cannot accept liability for the accessing of inappropriate materials or any consequences of internet access.

If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Headteacher immediately. Pupils are aware that they must only access those services they have been given permission to use.

Staff and pupils are made aware that the use of computer systems without permission or for inappropriate purposes is a criminal offence (Computer Misuse Act 1990) Staff must agree to and sign the Acceptable Use Agreement (see appendix) each year.

Log in and Passwords Pupils and staff must not disclose any password or login name given to anyone, or allow anyone else to use a personal account. Pupils and staff must not attempt to gain access to the school network or any Internet resource by using someone else's account name or password. Staff and pupils must ensure terminals or lap tops are logged off (or hibernated) when left unattended. Adult users are expected to be in charge of their own areas on the network. Passwords are therefore set for each user. We recommend that passwords are changed frequently. Passwords should be over 4 characters and should contain letters, numbers and symbols. They should not contain spaces.

General Safety and Risk Assessment

The consumption of food or drink is forbidden whilst using a computer. It is hazardous to the equipment and to individuals. Users must treat with respect equipment and services in school and at other sites accessed through school facilities, and are subject to regulations imposed by the respective service providers. Malicious action will result in immediate suspension from use of the school facilities. Staff are responsible for sharing the safety issues with their pupils.