Cedars Academy
E-Safety

Responsibility for Policy: SLG T&L
Date policy written/rewritten: February 2019
Dates policy reviewed: March 2020

Date: Spring 2019
Review date: Spring 2020

Ours is a community of learning, where secure partnerships create opportunities for students, staff, governors, parents and carers alike to participate and grow to become intellectually, emotionally and socially *fit for life.*

Introduction

The school's e-safety policy covers the safe use of the internet and electronic communications technologies and should be read in conjunction to the school's AUP (Acceptable Use Policy). It highlights the need to educate children and young people about the benefits and risks of using new technologies both in and away from school. It provides safeguards and rules to guide staff, pupils and visitors in their online experiences.

The e-safety policy will operate in conjunction with other policies including behaviour, curriculum, data protection, safeguarding children and home-school agreement.

Effective Practice

E-safety depends on effective practice in:
1. education for responsible ICT use by staff and pupils
2. a comprehensive, agreed and implemented e-safety policy
3. secure, filtered broadband from the Northern Grid for Learning
4. a school network that complies with the National Education Network standards and specifications.

Policy

The e-safety policy is part of the school development plan, is referred to in the SEF and relates to other policies on safeguarding, including those for ICT, behaviour and child protection.
The school has an e-safety co-ordinator. This is currently the AHT KS3&4. This is a non-technical role.

Teaching and Learning

The school internet access is designed for child and young person use and includes filtering appropriate to the age of pupils and access to safe search facilities as appropriate. Pupils are taught what internet use is acceptable and what is not. Access for staff may be at a different level to the children and the school will keep clear records of amendments to levels of filtering.

The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law.

Managing Internet Access

School ICT systems security will be reviewed regularly and improved. Virus protection will be updated regularly.

School e-mail addresses are not used for personal or private use. Staff and children may only use approved e-mail accounts on the school system. Staff and children must report if they receive offensive email. In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission. Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. Pupils' full names will not be used anywhere on a school web site or other on-line space, particularly in association with photographs. Written permission from parents or carers will be obtained before photographs of pupils are published on the school web site. Work can only be published with the permission of the pupil and parents/carers. Pupil image file names will not refer to the pupil by name. Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories – this policy will refer to where photos can be stored, how they can be accessed and when they will be destroyed.

The school will control access to social networking sites, and consider how to educate pupils in their safe use. Newsgroups will be blocked unless a specific use is approved. Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location. Staff, children and parents will be advised that the use of social networking spaces outside school brings a range of dangers. Staff should follow guidance not to have children as friends on social networking sites.

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. The SLG should note that technologies such as mobile phones with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications. Mobile phones will not be used during lessons or formal school time. Staff must not use their personal phones and cameras to record school activities. The sending of abusive or inappropriate text messages by Bluetooth or any other means is forbidden. The use by pupils of cameras in mobile phones will be kept under review. Games machines including the Sony PlayStation, Xbox and others have internet access which may not include filtering. Care is required in any use in school.

Some data may belong to the council (e.g. SIMS data). In this situation, the Academy would be classed as a 'data custodian' and would therefore need to seek permission from the Information Asset Owner, prior to sending that information (securely) to any third party. If the transfer of data is approved, then that transfer would be subject to a formal data sharing contract that ensures that the third party will adhere to the principles of the DPA.

SIMS

SIMS is accessible via a class PC. It is opened separately from network log-ins and is the responsibility of the teacher in charge (or delegated staff member). The school recommends the use of strong passwords and the teacher must ensure access is closed when away from the machine. There is no automatic log out in SIMS so teachers must be vigilant to ensure the system is closed. Authorised users will be added or removed by the office manager.

Policy Decisions

All staff must read and sign the staff AUP for ICT before using any school ICT resource. The school will maintain a current record of all staff and pupils who are granted access to the Academy systems. Parents will be asked to sign and return an AUP for their child. Any person not directly employed by the school will be asked to sign an 'acceptable use of academy ICT resources' before being allowed to access the internet from the school site. The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor Omnicom can accept liability for any material accessed, or any consequences of internet access. The Academy audits ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

Communications Policy

Pupils will be informed that network and internet use will be monitored and appropriately followed up. E-safety training will be embedded within the ICT scheme of work or the personal, social and health education (PSHE) curriculum. All staff will be given the school e-safety policy and its importance explained. Staff must be informed that network and internet traffic can be monitored and traced to the individual user. Staff will always use a child friendly safe search engine when accessing the web with pupils. Parents/carers attention will be drawn to the school e-safety policy and AUP in newsletters, the school brochure and on the school web site. The school will maintain a list of e-safety resources for parents/carers and promote these in various ways including the web and displays around the school.

Monitoring, Evaluation and Review

This policy will be reviewed annually.

Date policy written/rewritten: February 2019

DH