Cleves School
Learning Together

E-SAFETY POLICY

Reviewed on	May 2017
Reviewed by	Craig Smith
Review cycle	Annual
Next review date	Summer Term 2018

Writing and reviewing the E-safety policy

The Cleves E-safety Policy is part of the Strategic Plan and relates to other policies including those for ICT, Behaviour, Anti-Bullying and Safeguarding. Rebecca Flaherty is the Cleves ICT Coordinator and Ian Russ is the Child Protection Coordinator. The E-Safety Coordinator is Craig Smith

The Cleves E-safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior management and approved by governors. The E-safety Policy and its implementation will be reviewed biennially.

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
- Google Hub and Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Radio Broadcasting
- Music Downloading
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

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.

At Cleves School, 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 should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Policies are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as mobile phones, camera phones, PDAs and portable media players, etc).

Monitoring

Authorised ICT staff may inspect any ICT equipment owned or leased by the School at any time without prior notice. ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain School business related information; to confirm or investigate compliance with School policies, standards and procedures; to ensure the effective operation of School ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

ICT authorised staff may, without prior notice, access the e-mail or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

The school's ICT systems security will be reviewed regularly. Virus protection will be updated regularly by the Network Manager and security strategies will be discussed with Senior Management, ICT Coordinator and ICT support agencies. Forensic Software is in use and will monitor pupil's use of a computer in accordance with the Acceptable Use Policy. Any inappropriate used will be reported to the Child Protection Team.

Computer Viruses

All files downloaded from the Internet, received via e-mail or on removable media (e.g. memory stick, CD)

must be checked for any viruses using school provided anti-virus software before using them.

Never interfere with any anti-virus software installed on school ICT equipment that you use. If your machine is not routinely connected to the school network, you must make provision for regular virus updates through the ICT team.

If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact the School Business Manager or Deputy Headteacher immediately. They will advise you what actions to take and be responsible for advising others that need to know.

e-Mail and Google Hub

The use of e-mail within most schools is an essential means of communication for both staff and pupils. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an e-mail in relation to their age and good network etiquette; 'netiquette'.

The Google Hub is an integrated set of interactive online services that provide teachers, pupils and parents with information, tools and resources to support and enhance educational delivery and management. The school shows the children how to responsibly interact with one another via the Hub – showing respect, collaborating and communicating with each other. In the context of school, e-mail and the Hub should not be considered private.

- The school gives all staff their own e-mail account to use for all school business as a work based tool. This is to minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed. Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses.
- It is the responsibility of each account holder to keep the password to both their email and learning platform accounts secure.
- For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business.
- Children are taught how to successfully and safely use email and each child will be given their own personal Cleves School email address. Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- All pupil e-mail users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.
- Staff must inform the ICT coordinator or Deputy Headteacher if they receive an offensive e-mail.
- The forwarding of chain letters is not permitted.
- However the school e-mail is accessed, (whether directly, through webmail when away from the

office or on non-school hardware), all the school e-mail policies apply.

- Pupils must not arrange to meet any person that they have only ever previously met on the Internet or by email or in a chat room, unless a parent, guardian or teacher has given them permission and they take a responsible adult with them.
- Pupils must not place personal photos on any social network space provided in the school learning platform. Pupils will be advised to use nicknames and avatars when using social networking sites.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

E-safety

As E-safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named E-safety co-ordinator in this school is Craig Smith who has been designated this role as a member of the senior leadership team. All members of the school community have been made aware of who holds this post. It is the role of the E-safety co-ordinator to keep abreast of current issues and guidance.

Senior Management and Governors are updated by the Head/E-safety co-ordinator and all governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's acceptable use agreement is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PSHE

ICT and online resources are increasingly used across the curriculum. We believe it is essential for E-safety guidance to be given to the pupils on a regular and meaningful basis. E-safety is embedded within our curriculum and we continually look for new opportunities to promote E-safety.

- The school has a framework for teaching internet skills in ICT/ PSHE lessons.
- The school provides opportunities within a range of curriculum areas to teach about E-safety.
- Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the E-safety curriculum.
- Pupils are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.
- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modeling and activities.
- Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or CEOP report abuse button.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.

Internet Access

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

- The school maintains students who will have supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet technology.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.
- Users must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended restricted audience.
- Don't reveal names of colleagues, customers or clients or any other confidential information acquired through your job on any social networking site or blog.
- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the headteacher, network manager or ICT coordinator.
- It is at the Headteacher's discretion on what internet activities are permissible for staff and pupils and how this is disseminated.
- All staff have the right to request that a website be unblocked by the Network Manager for pupil use. It is the responsibility of the person requesting the website unblock to thoroughly check the website for inappropriate content.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the E-safety Coordinator.
- The child protection team will regularly check reports on inappropriate use of school computers.

Published Content and School Website

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device.
- The contact details on the Web site should be the school address, e-mail and telephone number.

Staff or pupils personal information will not be published.

- The Website Manager has overall editorial responsibility and ensures that content is accurate and appropriate; they do so with the support of other school staff.
- Publishing pupil's images and work:
- Pupils' full names will be avoided on the Web site or learning platform, as appropriate, including in blogs, forums or wikis, particularly in association with photographs.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.
- All pupils are supervised by a member of staff when video conferencing
- All pupils are supervised by a member of staff when video conferencing with end-points beyond the school
- The school keeps a record of video conferences, including date, time and participants.
- Approval from the Headteacher is sought prior to all video conferences within school.

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed
- Mobile phones and associated cameras will not be used during lessons or formal school time except as part of an educational activity. The sending of abusive or inappropriate text messages is forbidden.
- Games machines including the iPod Touch, iPad and other handheld consoles (e.g. Nintendo DS) have Internet access which may not include filtering. Care will be taken with their use within the school.
- Staff will use a school phone where contact with pupils or parents is required.

Communications

Pupils and the E-safety policy

Appropriate elements of the E-safety policy will be shared with pupils. Pupils will be informed that network and Internet use will be monitored. Curriculum opportunities will be provided for pupils to enable them to gain awareness of E-safety issues and how best to deal with them.

Staff and the E-safety policy

All staff are expected to familiarise themselves with the Cleves School E-safety Policy. Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting parents' support

Parents' and carer's attention will be drawn to the School E-safety Policy in newsletters, the school brochure and on the school web site. Parents and carers will from time to time be provided with additional information on E-safety. An E-safety presentation and workshop will be run annually which parents will be invited to attend. The school will also ask all new parents to sign the parent/pupil agreement when they register their child with the school.

Breaches

Complaints of Internet misuse will be dealt with by a senior member of staff. Any complaint about staff misuse must be referred to the appropriate line manager. Complaints of a child protection nature must be dealt with in accordance with Cleves school child protection procedures. Pupils and parents will be informed of consequences for pupils misusing the Internet.

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.

Any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure. Policy breaches may also lead to criminal or civil proceedings.

Reviewed: May 2017
By : C. Smith
Review date : May 2019
Govs Ref: WP