Policy: e-Safety Policy

Updated: February 2017
By: Mr Hugh Conway

Head Teacher: Mrs. Linda Rodham
Chair of Governors: Sue Saiger

Purpose

The purpose of this policy is to establish the ground rules we have in school for using ICT equipment and the Internet. We are also committed to educating students in the acceptable use of equipment, internet and new technologies and believe in educating and guiding rather than locking down equipment.

New technologies have become integral to the lives of children and young people in today's society, both within educational establishments and in their lives outside school. The Internet and other digital/information technologies are powerful tools which open up new opportunities for everyone.

Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe Internet access at all times. The requirement to ensure that children and young people are able to use the Internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound.

This e-safety policy will help to ensure safe and appropriate use. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school.

Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content.
- Unauthorised access to, loss of or sharing of personal information.
- The risk of being subject to grooming by those with whom they make contact on the Internet.
- The sharing/distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication/contact with others, including strangers.
- Cyber-bullying.
- Access to unsuitable video/Internet games.
- An inability to evaluate the quality, accuracy and relevance of information on the Internet.
- Plagiarism and copyright infringement.
- Illegal downloading of music or video files.
- The potential for excessive use which may impact on the social and emotional development and physical health impact on the young person.

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is read and used in conjunction with other school policies; specifically Anti-Bullying, Behaviour and Child Protection.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build pupils' resilience to the risks to which they may be exposed so that they have the confidence and skills to face and deal with these risks.

The school provides the necessary safeguards to help ensure that we have done everything that could reasonably be expected to manage and reduce these risks. The e-safety policy explains how the school intends to do this, whilst also addressing wider educational issues in order to help young people (and their parents/carers/staff) to be responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use.

Schools have a vital role to play in protecting children and young people from the risks of extremism and radicalization. This role is underpinned by the Counter Terrorism and Security Act (2015) to have due regard to the need to prevent people from being drawn into terrorism. The school has a clear Prevent Policy relating to this (please refer to this for more details). Students identified as possibly being a risk of radicalization will be referred as per agreed procedures and the school will work with other agencies to provide appropriate support. The school also seeks to reduce such risk through ensuring that a wide range of opportunities exist for the teaching (and learning) of Citizenship, Community Cohesion and British Values (e,g, through PSHCME program). Students engaging in school in any activities related to the Prevent Agenda will be sanctioned in accordance with the Behaviour for Learning Policy, as well as probable involvement with the Police.

Link to Other Policies

Schools have a vital role to play in protecting children not only on the "real" world but also in the "virtual" world. This role is underpinned by the school's approach to e-safety as outlined in the E-Safety Policy. Students are educated to keep safe on line via a range of strategies including CEOPS assemblies, our annual Internet Safety Week, ICT lessons, newsletters etc. The school's strategy for e-safety is scrutinised and monitored by our E-Safety Group, made up of teachers, students and governors. Students found to be using the internet/ICT for undesirable reasons including cyber bullying will be escalated through the school's consequence and sanction systems as detailed in the Behaviour for Learning Policy with possible involvement of the Police if this is deemed necessary (in serious cases). E-safety is covered by a range of school policies including the Behaviour for Learning Policy, Anti-Bullying Policy, E-Safety Policy, Prevent Policy, SMSC Policy and Child Protection Policy.

Teaching & Support Staff

In addition to elements covered in the Accessible Usage Policy (AUP), all teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e-safety policy and practices.
- They have read, understood and signed the school Acceptable Usage Policy (AUP).
- E-safety issues are embedded in all aspects of the curriculum and other school activities.
- Students understand and follow the school's e-safety and acceptable usage policies.
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold
- copyright regulations.
- They monitor ICT activity in lessons, extracurricular and extended school activities.
- In lessons where Internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that any unsuitable material that is found is reported to the ICT Network Team.
- They do not store any sensitive data on devices (USB memory sticks, portable hard drives, etc.) that are not encrypted.

It is recommended that:

- all data is stored on the school network and accessed remotely via the VLE
- If it is necessary to use a USB storage device, then it must be encrypted. School can supply encrypted memory sticks if required.

Students (to an age appropriate level)

- Are responsible for using the school ICT systems in accordance with the Acceptable Usage Policy, which they will be required to sign before being given access to school systems.

Parents/carers will be required

- to read through and sign alongside their child's signature.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and report these incidents using the 'Report it' button on the VLE.
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school, and realise that the school's e-safety policy also covers their actions out of school, if related to their membership of the school.

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use electronic devices appropriately. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take opportunities to help parents understand these issues. Parents and carers will be responsible for:

- Endorsing (by signature) the Acceptable Usage Policy.
- Monitoring of the students internet usage outside of school. Whilst in school we monitor and block inappropriate content but these systems are not available at home. So while we

endeavour teaching students what is acceptable, this message is vital at home where students have access to anything on the internet.

Commmunication

Email

- Digital communications with pupils (e-mail, online chat, VLE, etc.) should be on a professional level and only carried out using official school systems.
- Under no circumstances should staff contact pupils, parents/carers or conduct any school business using personal e-mail addresses.

Mobile Phones

- School mobile phones only should be used to contact parents/carers/students when on school business with students off site. Staff should not use personal mobile devices.
- Staff should not be using personal mobile phones in school during working hours when in contact with children.
- Students should adhere to the rules and guidelines set out in the Behaviour Policy regarding mobile phone use in school.

Social Networking Sites

Students will only be allowed on certain social networking sites at school to follow the activities as instructed by the teacher; at home it is the parents responsibility, but parents should be aware that it is illegal for children under the age of 13 to be on certain social networking sites.

Staff users should not reveal names of staff, pupils, parents/carers or any other member of the schoolcommunity on any social networking site or blog.

Staff/Students/Parents/Carers should be aware the school will investigate misuse of social networking if it impacts on the well-being of other students or stakeholders.

If inappropriate comments are placed on social networking sites about the school or school staff then advice would be sought from the relevant agencies, including the police if necessary.

Digital Images

The school record of parental permissions granted/not granted must be adhered to when taking images of our students. A list can also be obtained from the data office or the child protection officers in school.

Under no circumstances should images be taken using privately owned equipment without the express permission of the Head or the ICT Network Team.

Where permission is granted the images should be transferred to school storage systems and deleted from privately owned equipment at the earliest opportunity.

Although many of the above points are preventative and safeguarding measures, it should be noted that the school will endeavour whenever possible to use social networking in positive ways to publicise, inform and communicate information. The school has active Facebook and Twitter accounts which are used to inform, publicise school events and celebrate and share the achievementof students.

Monitoring

All use of the school's Internet access is logged and the logs are regularly monitored. We also use a system that logs any misuse, bad language, etc. that happens on any of the school's equipment. Whenever any inappropriate use is detected it will be followed up by the schools ICT Network Team.

The ICT Network Team will keep a log of all e-safety transgressions. This also lists the outcomes of any investigations and consequences that have been applied.

Any member of staff employed by the school who comes across an e-safety issue does not investigate any further, but immediately reports it to the ICT Network Team and confiscate/impounds the equipment. If the concern involves the ICT Network Team then the member of staff should report the issue to the Head.

Incident Reporting

Any e-safety incidents must immediately be reported to the ICT Network Team . Students can also use the 'Report it' button on the VLE to log any issues. There are also links to the CEOPS website from the school website and the VLE.

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place through careless or irresponsible, or very rarely, through deliberate misuse. If any apparent or actual, misuse appears to involve illegal activity e.g. child sexual abuse images, adult material which potentially breaches the Obscene Publications Act, criminally racist material or other criminal conduct, activity or materials, the ICT Network Team or Headteacher should be informed.

Actions will be followed in accordance with policy, in particular the sections on reporting the incident to the police and the preservation of evidence. If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. It is recommended that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer. It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures.

Acceptable Use Policies

Refer to the the individual policies listed below:

- Student ICT Acceptable Use Policy
- Staff ICT Acceptable Use Policy
- iPad Acceptable Use Policy