TWYCROSS HOUSE SCHOOL

Policy on E-safety

Introduction

Twycross House School recognises that, within the context of a range of teaching and learning methods and face to face interaction, ICT offers a wide range of opportunities and that access to ICT both at school and at home is universal and increasingly more mobile. Furthermore, in light of the ongoing Covid pandemic, the integration of classroom based and at-home ICT use has become a necessity.

E-safety is the school's ability to protect and educate pupils and staff in their safe and appropriate use of ICT and to have the mechanisms to intervene and support any incident as necessary. The 'Keeping Children Safe in Education' guidelines (2023) state that 'It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate' This policy aims to show how the school facilitates this.

Aims of the Policy

- To provide practical guidance and clear procedures for ensuring that ICT is used in an appropriate, safe way.
- To maintain the school's high standards of child protection by ensuring that pupils and staff are aware of appropriate ICT use.
- To give effective support, guidance and information to teachers, pupils and parents on issues surrounding e-safety.

Roles and Responsibilities

The Headmaster has overall responsibility for the safety (including e-safety) of staff and pupils. However, the day to day running of e-safety is designated to the e-safety co-ordinator, Mrs Sanganee and responsibility for child safeguarding issues and overall provision of e-safety to Mr Knight. The Headmaster is, however, responsible for:

- Ensuring that staff use of ICT, including mobile phones and social media both inside and outside (where it concerns the school and its community) of school is appropriate.
- Dealing with incidences of misuse with regards to the above.

Mr Knight is the senior designated member of staff in charge of child safeguarding. Any e-safety related matter which is considered to be a child safeguarding issue will be reported to him as per the school child safeguarding policy. He is responsible for producing the ICT Code of Practice for Teachers and Adults. He is aware of e-safety issues and the potential for serious incidents arising from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults /strangers
- Potential or actual incidents of grooming
- Cyber-bullying

(The school aims to prevent and respond to cyberbullying. Please refer to the cyberbullying section of the Anti-bullying Policy)

Mrs Sanganee is the nominated e-safety co-ordinator. She has received training in the provision of e-safety guidance in schools having attended the CEOP 'Thinkuknow' Introduction course. She is responsible for:

- Writing the e-safety policy and ensuring that it is updated as necessary to ensure its relevance with regards to changing technologies.
- Writing and delivering the e-safety curriculum to pupils.
- Raising awareness of e-safety issues to pupils, staff and parents.

Mr Westaway is head of computing. He will support Mrs Sanganee in any technological aspects of delivering the e-safety curriculum and is also responsible for:

- Creating the acceptable use policy.
- Ensuring that only permitted persons have access to computers via a properly enforced password protection policy.
- Ensuring that the school's technological infrastructure is adequately protected from misuse and that effective filtering of internet sites is in place.
- Reinforcing the e-safety message via ICT lessons.

Teachers have a responsibility to act as good role models to pupils in their use of ICT, social media and mobile devices. They are aware of child safety guidelines with regards to acceptable use of ICT, including social media and mobile phones. They are also responsible for:

- Monitoring the use of mobile devices e.g. phones, cameras in lessons and around school and dealing with any misuse appropriately as outlined below.
- Considering online safety whilst planning the curriculum.
- Ensuring that pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Educating pupils in matters regarding e-safety through their role as form teacher or in the teaching of their own subject.
- Managing and/or reporting e-safety related incidents e.g. pupil misuse of ICT, cyberbullying, plagiarism etc.

All adults and teachers working at the school must comply with the school's ICT Code of Practice for Teachers and Adults.

Pupils play a key part in ensuring that their use of ICT both inside and outside of lessons at school and at home is a positive experience. They are responsible for:

- Adhering to the school policies with regard to computer and electronic device use and following instructions given by teachers relating to this.
- Being aware that school e-safety rules are applicable to use of computers and electronic devices at home if it is related to their membership of the school.
- Knowing the importance of reporting abuse, misuse or accessing inappropriate behaviour and how to do so.

Parents have a role to play in supporting the school's e-safety policy by:

- Reinforcing the importance of appropriate and safe ICT use at home and at school.
- Agreeing to the terms of the school acceptable use policy and mobile phone use policy.

Statutory Responsibilities

In the event of suspicion of serious misuse of ICT by any member of the school community, the school has a statutory responsibility to carry out all steps of the following procedure:

- Have more than one senior member of staff/volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed and signed (except in the case of images of child sexual abuse – see below).
- Once this has been completed and fully investigated the school will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:

- Internal response or discipline procedures
- Involvement by Local Authority or national / local organisation (as relevant)
- Police involvement and/or action

If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the police immediately. Other instances to report to the police would include:

- Incidents of ‘grooming’ behaviour
- The sending of obscene materials to a child

- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Other criminal conduct, activity or materials

The computer in question must be isolated as effectively as possible, as any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. Any documentation should be retained by the group for evidence and reference purposes.

Dealing with Problems

In addition to the statutory responsibilities outlined above, the following steps should be taken when incidents of misuse of ICT occur:

- If a mobile phone, camera or other electronic device is used inside of lessons this should be removed from the pupil and taken to reception for collection at the end of the day. Repeat occurrences of this should be reported to form-teachers, Mr Assinder/Mr Knight and parents and will result in sanctions which may include denying the pupil permission to bring a mobile phone into school.
- If any of the above devices are being used inappropriately around the school outside of lessons the incident should be dealt with as above.
- If pupils or parents have a concern about cyber-bullying or any other misuse of ICT use in school or outside of school (if it relates to their membership of the school community) they should speak to the form tutor, or another adult with whom they feel comfortable. This will be managed in accordance with the school cyber-bullying policy.
- If a pupil is behaving in a way that contravenes the acceptable use policy whilst using the ICT room, the pupil should be removed from the computer for the rest of the lesson (ensure that the computer is left as it was when the incident occurred) and the incident reported to Mr Westaway to allow her to make any technical assessment of the incident. This should then be referred to the form tutor and Mr Assinder/Mr Knight and parents depending on the severity of the incident. Appropriate sanctions will be imposed in accordance with the school behaviour and sanctions policy.

Delivering the E-safety Message to Pupils

Educating pupils in e-safety is the main aspect of the school's e-safety provision. In line with Ofsted recommendations, we endeavour to help and support pupils in being able to recognise and manage the risks of ICT so that they are able to use it responsibly in both their school and home life.

In line with the 'Keeping Children Safe in Education' guidelines (2023) the e-safety provision at Twycross House School is based on the following 4 areas:

- **content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

- **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.

- **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and

- **commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams

The school delivers this e-safety message in the following ways:

- E-safety is part of the whole curriculum and staff should reinforce e-safety messages as they arise in their own teaching.
- An e-safety curriculum which delivers age-appropriate guidance on the safe and responsible use of ICT is delivered through assemblies and activities in form time.
- In lessons/homework where internet use is pre-planned, pupils will be guided towards sites that are suitable for their use.
- Where pupils are allowed to freely search the internet in lessons, teachers will be vigilant in monitoring the content of the websites that pupils visit and will ensure that pupils are not accessing other sites, e.g. social media during the lesson.
- Pupils will be taught in all lessons to be critically aware of the materials that they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Staff

- E-safety issues will be included in the whole-school Child Safeguarding training.
- Teacher training for new staff will include e-safety information

Mr Knight
Updated September 2023