E-Safety and IT Acceptable Use Policy

Wotton House International School

CONTENTS

1. Rationale

It is our duty to take responsibility for the safety and appropriate use of technology in our organisation. Our starting point is that our students must understand where the boundaries of appropriate uses of technology lie and where they might be vulnerable to inappropriate online content, contact or conduct. Respecting others is at the heart of our philosophy and extends into the digital domain.

1. The Internet and digital technologies allow all those involved in education to promote creativity, collaboration, stimulate global awareness, to teach online safety and resilience and to enhance the learning experience.
2. As part of our commitment to learning in a safe environment, we want to ensure that the Internet and other digital technologies are used to:
    1. raise educational standards and promote student achievements;
    2. develop the curriculum and make learning engaging and purposeful;
    3. enable students to gain access to a wide span of knowledge in a way that ensures their safety;
    4. develop students' skills of cooperation, collaboration, resilience and competition;
    5. prepare our students to be effective 21st century citizens.
    6. train and educate the school community about appropriate use of online technologies and safety risks.
3. The latest resources promoted by the DfE can be found at: The UK Safer Internet Centre (www.saferinternet.org.uk) and CEOP's Thinkuknow website (www.thinkuknow.co.uk)

2. Teaching and Learning

1. The Internet is an essential element in 21st century life for education, collaboration, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
    1. Internet use is a part of the curriculum and a necessary tool for staff and students.
    2. Our Internet access is designed expressly for staff and students to use and includes filtering appropriate to the age of students.
    3. Students are taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
    4. Students are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
2. **School E-safety Strategies**. We make every reasonable effort to ensure unsavory or illegal websites are blocked but no system is 100% reliable and, as such, we rely on the cooperation of our staff and students to report any issues discovered. The risk associated with use of ICT by children can be grouped into 4 categories, as follows.
    1. **Content**. The internet contains a vast store of information from all over the world which is mainly aimed at an adult audience and may be unsuitable for children. There is a danger that children may be exposed to inappropriate images such as pornography, or information advocating violence, racism or illegal and anti-social behaviour that they are unable to evaluate in a critical manner.
    2. **Contact**. Chat rooms and other social networking sites can pose a real risk to children as users can hide their true identity. The sites may be used by adults who pose as children in order to befriend and gain children's trust (known as "grooming") with a view to sexually abusing them. Children

may not be aware of the danger of disclosing personal information about themselves such as contact details that allow them to be identified or located. They may also inadvertently put other children at risk by posting personal information and photographs without consent. The internet may also be used as a way of bullying a child, known as cyberbullying.

3. **Commerce**. Children are vulnerable to unregulated commercial activity on the internet that could have serious financial consequences for themselves and their parents. They may give out financial information, for example, their parent's credit card details or in app purchases, in response to offers for goods or services without seeing the fraudulent intent. Disclosing this information can lead to fraud or identity theft.
4. **Culture**. Children need to be taught to use the internet in a responsible way, as they may put themselves at risk by:
    - becoming involved in inappropriate, antisocial or illegal activities as a result of viewing unsuitable materials or contact with inappropriate people
    - using information from the internet in a way that breaches copyright law
    - uploading personal information about themselves on social networking sites without realising they are publishing to a potentially global audience
    - Cyberbullying
    - Hacking
    - Children may also be adversely affected by obsessive use of the internet that may have a negative impact on their development and educational attainment.

3. **Roles and responsibilities**. A successful e-safety strategy needs to involve the whole school community and forge links with parents and carers. The strategy should be overseen by the Principal, IT Manager and be fully implemented by all staff, including technical and non-teaching staff.

    1. Principal's role. The Principal has ultimate responsibility for e-safety issues within the school including:
        - the overall development and implementation of the school's e-safety policy
        - ensuring that e-safety issues are given a high profile within the school community
        - linking with senior management, parents and carers to promote e-safety
        - ensuring e-safety is embedded in the curriculum
        - deciding on sanctions against staff and students who are in breach of acceptable use policies.

    2. IT Manager's role. Given the issues associated with e-safety, it is appropriate for the DSL to work alongside the IT Manager who has the authority, knowledge and experience to carry out the following:
        - develop, implement, monitor and review the school's e-safety policy
        - ensure that staff and students are aware that any e-safety incident should be reported to them
        - provide the first point of contact and advice for school staff, students and parents
        - keep up-to-date with e-safety issues and advise of any new trends, incidents and arising problems to the Principal
        - assess the impact and risk of emerging technology and the school's response to this
        - raise the profile of e-safety awareness within the school by ensuring access to training and relevant e-safety literature
        - ensure that all staff and students have read and signed the acceptable use policy
        - report annually to the Principal on the implementation of the school's e-safety strategy
        - maintain a log of internet related incidents and coordinate any investigation into breaches
        - carry out monitoring and audits of networks and reporting breaches to the Principal.
        - support any subsequent investigation into breaches and preserve any evidence.

    3. Role of school staff. Teaching staff have a dual role concerning their own internet use and providing guidance, support and supervision for students. Their role is:
        - adhering to the school's e-safety and acceptable use policy
        - communicating the school's e-safety and acceptable use policy to students
        - keeping students safe and ensuring they receive appropriate supervision and support whilst using the internet
        - planning use of the internet for lessons and researching online materials and resources
        - reporting breaches of internet use to the IT Manager
        - recognising when students are at risk from their internet use or have had negative experiences and taking appropriate action, for example referral to the IT Manager.

    4. Designated Safeguarding Lead. Where any e-safety incident has serious implications for the child's

safety or well-being, the matter should be referred to the DSL who will decide whether or not a referral should be made to the Local Area Designated Officer (LADO) or the Police.

4. **Students with special needs**. Students with learning difficulties or disability may be more vulnerable to risk from use of the internet and will require additional guidance on e-safety practice as well as closer supervision. SEN co-ordinators are responsible for providing extra support for these students and should:
    - link with the IT Manager to discuss and agree whether the mainstream safeguarding systems are adequate for students with special needs.
    - where necessary, liaise with the IT Manager to discuss any requirements for further safeguards or tailored resources and materials in order to meet the needs of students with special needs
    - ensure that the school's e-safety policy is adapted to suit the needs of students with special needs.
    - liaise with relevant agencies in developing e-safety practices for students with special needs
    - keep up to date with any developments regarding emerging technologies and e-safety and how these may impact on students with special needs.

5. **Working with parents and carers**: It is essential that schools involve parents and carers in the development and implementation of e-safety strategies and policies; most children will have internet access at home and might not be as closely supervised in its use as they would be at school
    - Parents and carers need to know about the risks so that they are able to continue e-safety education at home and regulate and supervise children's use as appropriate to their age and understanding
    - The Principal and IT Manager should consider what strategies to adopt in order to help parents be aware of e-safety issues and support them in reinforcing e-safety messages at home.
    - Parents should be provided with information on ICT learning and the school's e-safety policy when they are asked to sign acceptable use agreements on behalf of their child so that they are fully aware of their child's level of internet use within school as well as the school's expectations regarding their behaviour.

3. E-Safety Procedures

1. Accessing and monitoring the system
    1. If students use a school computer, they are able to set their own passwords; staff access is through their own personal accounts.
    2. The school takes no responsibility for damage to personal devices. The same conduct use terms that apply to school netbooks also apply to personal devices.
    3. The IT Manager has access to all computers and can access all logins used within the school for the purposes of monitoring and auditing internet activity conducted via the school internet connection.
2. **Acceptable use policies** Staff must sign an acceptable use policy on appointment. The school office will keep a copy of all signed acceptable use agreements.
3. Teaching e-safety
    1. Responsibility. One of the key features of the school's e-safety strategy is teaching students to protect themselves and behave responsibly while online. There is an expectation that over time, students will take increasing responsibility for their own behaviour and internet use so that they can be given more freedom to explore systems and applications with a lessening amount of supervision from staff.
    2. Content. Students will learn:
        - the benefits and risks of using the internet
        - how their behaviour can put themselves and others at risk & what strategies they can use to keep themselves safe
        - what to do if they are concerned about something they have seen or received via the internet & who to contact
        - that the school has a "no blame" policy so that students are encouraged to report any e-safety incidents so that mistakes allow an opportunity to learn in a supportive environment.
        - that the school has a "no tolerance" policy regarding cyberbullying
        - behaviour that breaches acceptable use policies will be subject to sanctions
        - school internet should only be used for educational purposes
        - the school system has been designed so that use is monitored and that access to some sites are blocked
        - the school's policy on using their own mobile phones whilst in school.
    3. Delivering e-safety messages
        - Teachers are primarily responsible for delivering an ongoing e-safety education in the classroom as part of the curriculum.
        - Rules regarding safe internet use are posted around the school to make students aware of any risks and reporting protocols.
        - The start of every lesson where computers are being used is an opportunity to remind

students of expectations on internet use and the need to follow basic principles to keep safe.
- Teachers use PSHE lessons as a forum for discussion on e-safety issues to ensure that students understand the risks and why it is important to regulate their behaviour whilst online.
- Teachers should be aware of those children who may be more vulnerable to risk from internet use, generally those children with a high level of experience and good computer skills but coupled with poor social skills.
- Teachers should ensure that the school's policy on students' use of their own mobile phones in school is adhered to.

4. ICT and safe teaching practice. Staff are made aware through induction and ongoing training, of the importance of maintaining professional standards of behaviour with regards to their own internet use, particularly in relation to their communications with students.
    - Photographs of students should only be taken by staff in connection with educational purposes.
    - No photographic or video images related to school should be transferred to a third person without permission being granted by the employee's line manager or a member of the senior management team.
    - Staff should take care regarding the content of and access to their own social networking sites.
    - Staff should be particularly careful regarding any comments to do with the school or specific students..
    - Staff should not engage in any conversation with students via instant messaging or social networking sites as these may be misinterpreted or taken out of context.
    - Where staff need to communicate with students regarding school work, this should be via school email.
    - When making contact with parents or students by telephone, staff should only use school equipment.
    - Staff should ensure that personal data relating to students is stored securely.
    - Where staff are using mobile equipment such as laptops provided by the school, they should ensure that the equipment is kept safe and secure at all times.
5. Evaluating and using internet content As the information generated by internet searches could be vast, and much of it irrelevant to the subject being taught, teachers should teach students good research skills that help them to maximise the resource. They should also be taught how to critically evaluate the information retrieved by:
    - questioning the validity of the source of the information; whether the author's view is objective and what authority they carry
    - carrying out comparisons with alternative sources of information
    - considering whether the information is current and whether the facts stated are correct.
    - In addition, students should be taught the importance of respecting copyright and correctly quoting sources and told that plagiarism (copying other's work without giving due acknowledgement) is against the rules of the school and may lead to disciplinary action.

4. Specific Technologies.

1. **Emails**: We use Google Apps for Education email to communicate with staff and students.
    - Emails should only be sent via Google Apps for professional and educational purposes only.
    - Students should be taught not to disclose personal contact details for themselves or others such as addresses or telephone numbers via email correspondence.
    - All email communications should be polite; if a student receives an offensive or distressing email, they should be instructed not to reply and to notify the responsible teacher immediately.
    - Students should be warned that bullying or harassment via email will not be tolerated and will be dealt with in accordance with the school's anti-bullying policy.
    - All students should be issued with an individual account using their login and password.
    - Students must be taught that all email messages sent using the school systems may be reviewed by the school as and when the school feels the need to do so.
    - Students should be taught to send as few attachments as possible and to use more appropriate file transfer technologies. They must be taught to be wary of opening attachments to emails where they are unsure of the content or have no knowledge of the sender.
2. **Social networking** sites such as Facebook, Instagram, Twitter and Tumblr allow users to publish information about them to be seen by anyone who has access to the site. The use of these sites is not prohibited, but is not to be used during class time without teacher permission. **Newsgroups and forums** are sites that enable users to discuss issues and share ideas online.
    1. Access to unregulated public social networking sites, newsgroups or forums may be blocked by the school filter. Students must be taught to be aware of the dangers of using such sites.
    2. Where schools identify a clear educational use for these sites for online publishing, they should use professional judgment and ensure that:

- Any use of these sites should be carefully supervised by the responsible teacher.
- Students should be warned that any bullying or harassment via social networking sites will not be tolerated and will be dealt with in accordance with the school's anti-bullying policy.

3. In order to teach students to stay safe on social networking sites, they should be advised: not to give out personal details to anyone online that may help to identify or locate them or anyone else, for example home address, name of school or clubs attended
4. not to upload inappropriate or revealing personal photos of themselves or others onto sites and to take care regarding what information is posted:
    - how to setup security and privacy settings on sites or use a "buddy list" to block unwanted communications or deny access to those unknown to them
    - to behave responsibly whilst online and to keep communications polite
    - not to respond to any hurtful or distressing messages but to let their parents, carers or IT Manager know so that appropriate action can be taken.

3. **Chat rooms and instant messaging**. Chat rooms are internet sites where users can join in "conversations" online; instant messaging allows instant communications between two or more people online. In most cases, students will use these at home although the school filter does block some of these applications.
    1. Inappropriate or adult chat rooms may be blocked by the school filter where it is possible to do so, however many services such as instant messaging apps may not blocked on student's personal devices.
    2. Students should be warned that any bullying or harassment via chat rooms or instant messaging taking place within or out of school will not be tolerated.
    3. To teach students to stay safe whilst using chat rooms outside of school, they should be advised:
        - not to give out personal details to anyone online that may help to identify or locate them or anyone else (disable geo positioning)
        - use moderated chat rooms that require registration and are specifically for their age group
        - not to arrange to meet anyone whom they have only met online
        - to behave responsibly whilst online and keep communications polite
        - not to respond to any hurtful or distressing messages but to let their an adult know so that appropriate action can be taken.
4. **Video conferencing**. This enables several users to communicate face-to-face via the internet using web cameras.
    - Video conferencing during school time should only be used for educational purposes.
    - Teachers should avoid using other webcam sites on the internet due to the risk of them containing links to adult material. In the event that teachers do use other webcam sites, this should be discussed and agreed in advance with the IT Manager and appropriate training given.
    - Student use of video conferencing should be for educational purposes and should be authorised & supervised as appropriate to their age.
    - Teachers should ensure that students are appropriately dressed during any photography or filming and equipment must not be used in changing rooms or toilets.
5. **School website**
    - Content uploaded onto the school website must be accurate, suitable for the purpose and audience, and not in breach of copyright or intellectual property law.
    - The marketing manager and Administrator or other persons designated by the Principal have responsibility for uploading marketing and administrative materials onto the school website. Management have responsibility for overseeing the content and upload of educational materials.
    - Staff school email addresses may be published to allow parents to contact teachers.
    - No personal contact details for students should be contained on the website and children's full names should never be published on the website.
    - Links to any external websites should be regularly reviewed to ensure that their content is appropriate for the school and the intended audience.
6. **Photographic and video images**
    - Where the school uses photographs and videos of students for publicity purposes, for example on the school website, images should be carefully selected so that individual students cannot be easily identified. It is recommended that group photographs are used.
    - Where photographs or videos of children are used and their image may be recognizable, written permission must be obtained first from their parents or carers, who should be informed of the purpose of the image and where it will appear.
    - Only student's first names should be published where their photograph or video is being used. Staff should ensure that children are suitably dressed to reduce the risk of inappropriate use of images
    - Images should, where practical, be securely stored only on the school's computer system and all other copies deleted. If personal equipment is used to take videos or images of students the content needs to be deleted from the staff member's equipment promptly. For ongoing projects where film or images are involved staff are encouraged to make use of school filming or camera equipment. Any exceptions to this rule must be discussed with the Principal.

- Stored images should not be labelled with the child's name and all images held of children should be deleted once the child has left the school.

7. Students own mobile phone/handheld devices

- The majority of students are likely to have mobile phones or other equipment that allows them to access internet services.
- The use of mobile phones during class is not allowed unless a teacher gives direct permission. Calls from parents are not allowed to be answered during class times and emergency calls should be made via the reception desk.
- Students may use their tablets or laptops for school work and need to comply with the acceptable use policy.
- Students must, if requested, set the language of their computer to English to allow their work to be supported by staff..
- Students and teachers are not allowed to take any photos in or around the toilets.
- Students may not video or photograph teachers with their personal devices. If a student is making a school video, a school device needs to be used and content only used for school work**.**

5. Responding To Incidents

1. Policy statement
    1. All incidents and complaints relating to e-safety and unacceptable internet use will be reported to the IT Manager in the first instance and recorded on the e-safety incident report form.
    2. Where the incident relates to a member of staff, the matter must always be referred to the Principal.
    3. The IT Manager keeps a log of all e-safety incidents and complaints and regularly review the information for evidence of emerging patterns of individual behaviour or weaknesses in the school's e-safety system, and use these to update the e-safety policy.
    4. E-safety incidents involving safeguarding issues, for example contact with inappropriate adults, should be reported to the DSL, who will make a decision as to whether or not to refer the matter in conjunction with the Principal.
    5. Although it is intended that e-safety strategies and policies should reduce the risk to students whilst online, this cannot completely rule out the possibility that students may access unsuitable material on the internet. We cannot accept liability for material accessed or any consequences of internet access, but all reasonable precautions will be taken to ensure a safe e-learning environment. Mistakes are unavoidable and should be used as a learning opportunity when they do happen.
2. Unintentional access of inappropriate websites
    1. If a student or teacher accidentally opens a website that has content which is distressing or upsetting or inappropriate to the students' age, teachers should immediately close or minimise the screen.
    2. Teachers should reassure students that they have done nothing wrong and discuss the incident with the class to reinforce the e-safety message and to demonstrate the school's "no blame" approach.
    3. The incident should be reported to the IT Manager and details of the website address and URL provided.
    4. The IT Manager should ensure that access to the site is blocked and the school's filtering system reviewed to ensure it remains appropriate.
    5. It is essential that teachers ensure that where they have asked for filtering to be lifted for a particular lesson (eg: sex education) that they notify the School IT team so that filtering can be put back to minimise the risk of inappropriate sites being accessed by students or staff
3. Intentional access of inappropriate websites by a student
    1. If a student deliberately accesses inappropriate or banned websites, they will be in breach of the acceptable use policy and subject to appropriate sanctions.
    2. The incident should be reported to the IT Manager and details of the website address and URL recorded.
    3. The IT Manager should ensure that access to the site is blocked.
    4. The student's parents should be notified of the incident and what action will be taken.
    5. This will be regarded as an opportunity to address a potential safeguarding issue.
4. Inappropriate use of ICT by staff
    1. If a member of staff witnesses misuse of ICT by a colleague, they should report this to the Principal and the IT Manager immediately.
    2. The IT Manager should ensure that the computer or laptop is taken out of use and securely stored in order to preserve any evidence, recording any action taken.
    3. The IT Manager should carry out an audit of use to establish which user is responsible and the details of materials accessed.
    4. Once the facts are established, the senior management team should take any necessary disciplinary action against the staff member and report the matter to the Proprietor and the police where appropriate.
    5. If the materials viewed are illegal in nature the Principal should report the incident to the police and follow their advice, which should also be recorded.
5. **Cyberbullying** is defined as the use of ICT to deliberately hurt or upset someone. Unlike physical forms of

bullying, the internet allows bullying to continue past school hours and invades the victim's home life and personal space. It also allows distribution of hurtful comments and material to a wide audience.

1. Cyberbullying is prevalent as students who would not consider bullying in the physical sense may find it easier to bully through the internet, especially if it is thought the bullying may remain anonymous
2. Bullying may take the form of:
    - rude, abusive or threatening messages via email or text
    - posting insulting, derogatory or defamatory statements on blogs or social networking sites
    - setting up websites that specifically target the victim
    - making or sharing derogatory or embarrassing videos of someone via mobile phone or email
3. Cyberbullying can affect students and staff members. Often, the internet allows the bully to remain anonymous. In extreme cases, cyberbullying could be a criminal offence under the Harassment Act 1997 or the Telecommunications Act 1984.
4. Dealing with incidents.
    1. Our anti-bullying and behaviour policies and acceptable use policies cover the issue of cyberbullying and set out clear expectations of behaviour and sanctions for any breach.
    2. Any incidents of cyberbullying should be reported to the IT Manager who will record the incident and ensure that the incident is dealt with in line with the school's anti-bullying policy. Incidents should be monitored and the information used to inform the continuous development of anti-bullying policies.
    3. Where incidents are extreme, for example threats against someone's life, or continue over a period of time, consideration should be given to reporting the matter to the police as in these cases, the bullying may be a criminal offence.
    4. As part of e-safety awareness and education, students should be told of the "no tolerance" policy for cyberbullying and encouraged to report any incidents to their teacher.
    5. students should be taught:
        - to only give out mobile phone numbers, social networking identifiers and email addresses to people they trust
        - to only allow close friends they trust to have access to their social networking page
        - not to respond to offensive messages
        - to report the matter to their parents and teacher immediately.
    6. Evidence of bullying, for example texts, emails or comments on websites should be preserved by the young person as evidence.
5. Action by service providers. All website providers and mobile phone companies are aware of the issue of cyberbullying and have their own systems in place to deal with problems, such as tracing and blocking communications. Teachers or parents can contact providers at any time for advice on what action can be taken.
    - Where the bullying takes place by mobile phone texts, the mobile phone company can be contacted to ask them to trace the calls and ensure that any further calls and texts from that number are blocked. The student should also consider changing their phone number.
    - Where the bullying takes place by email, and the messages are being sent from a personal email account, contact the service provider so that the sender can be traced and further emails from the sender blocked. The student should also consider changing email address.
    - Where bullying takes place in chat rooms, the student should leave the chat room immediately and seek advice from parents or teachers. Bullying should be reported to any chat room moderator to take action.
    - Where bullying involves messages on social networking sites or blogs, contact the website provider to request that the comments are removed. In extreme cases, the bully's access to the site can be blocked.
    - Parents should be notified of any incidents and advised on what measures they can take to block any offensive messages on computers at home.
6. Cyberbullying of teachers by students. Because of the duty of care owed to staff, the Principal should ensure that teachers are able to report incidents in confidence and receive adequate support, including taking any appropriate action against students.
    - Incidents of cyberbullying involving teachers should be recorded and monitored by the IT Manager in the same manner as incidents involving students.
    - Teachers should follow the guidance on safe ICT use in this policy and avoid using their own mobile phones or email addresses to contact parents or students so that no record of these details becomes available.
    - Personal contact details for teachers should not be posted on the school website or in any other school publication.
    - Teachers should follow the advice above on cyberbullying of students and not reply to

messages but report the incident to the Principal immediately.

6. **Risk from inappropriate contacts**. Staff may be concerned about a student being at risk as a consequence of their contact with an adult they have met over the internet. The student may report inappropriate contacts or staff may suspect that the student is being groomed or has arranged to meet with someone they have met online.
    - All concerns around inappropriate contacts should be reported to the IT Manager and the DSL.
    - The DSL should discuss the matter with the referring teacher and where appropriate, speak to the student involved, before deciding whether or not to make a referral.
    - The police should always be contacted if there is a concern that the child is at immediate risk, for example if they are arranging to meet the adult after school.
    - Teachers should advise the student how to terminate the contact and change contact details where necessary to ensure no further contact.
    - The DSL and IT Manager should always notify the student's parents of any concerns or incidents and where appropriate, arrange to meet with them to discuss what action they can take to ensure their child's safety.
    - Where inappropriate contacts have taken place using school ICT equipment or networks, the IT Manager should make a note of all actions taken and ensure that all evidence is preserved and that an audit of systems is carried out to ensure that the risk to other students is minimised.
7. **Staff - student contact**. Staff should only use WHIS email accounts or WHIS social media platforms to communicate with current or former students.
    1. Staff should not accept student requests or make requests for communication on any personal social media platforms.
    2. If a staff member has accidentally allowed contact with a student online/digitally, the staff member involved should report it immediately to the IT Manager and DSL.
    3. Students should not "follow" or sign up to any staff member's personal/non professional online social media accounts and staff should be aware of the anonymous nature of various social media systems. If a staff member notices the above they should block the student and report it to the IT Manager.
    4. Staff and students should only contact each other through the school email system.
8. Risk from contact with violent extremists. Many extremist groups use the internet as a means of either inciting violence against specific groups or providing information on preparing explosives or carrying out terrorist acts. Because of their personal circumstances, some young people may be susceptible to these influences
    1. Staff need to be aware of those students who are being targeted by or exposed to harmful influences from violent extremists via the internet. students and staff are warned of the risks of becoming involved in such groups and informed that accessing such websites is against school policies
    2. We ensure that adequate filtering is in place and review filtering in response to any incident where a student or staff member accesses websites advocating violent extremism.
    3. All incidents should be dealt with as a breach of the acceptable use policies and the school's behaviour and staff disciplinary procedures should be used as appropriate.
    4. The IT Manager and DSL should record and review all incidents in order to establish whether there are any patterns of extremist groups targeting the school and whether current school procedures are robust enough to deal with the issue.

6. SANCTIONS FOR MISUSE OF SCHOOL ICT

1. Student Category A infringements. These are continued serious breaches of acceptable use following warnings or deliberately accessing and distributing banned/ illegal materials which may result in a criminal offence, such as:
    1. persistent and/or extreme cyberbullying
    2. deliberately accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
    3. receipt or transmission of material that infringes copyrights or is in breach of the Data Protection Act
    4. bringing the school name into disrepute.

    Sanctions could include: referral to Principal; contact with parents; possible exclusion; removal of equipment; referral to community police officer
2. Student Category B infringements. These are deliberate actions that either negatively affect the school IT system or are serious breaches of acceptable use agreements or anti-bullying policies, such as:
    1. deliberately bypassing security or access
    2. deliberately corrupting or destroying other people's data or violating other's privacy
    3. Cyberbullying
    4. deliberately accessing, sending or distributing offensive or pornographic material
    5. purchasing or ordering items over the internet
    6. transmission of commercial or advertising material

    Sanctions could include: referral to class teacher or tutor; referral to Principal; loss of access to internet

use for a period of time; contact with parents; any sanctions agreed under other school policies

3. Student Category C infringements. These are persistent breaches of acceptable use agreements following warnings and use of banned sites or serious breaches of e-safety policy that are non-deliberate, such as:
    1. continued use of non-educational sites during lessons
    2. continued unauthorized use of email or mobile phones
    3. continued use of prohibited sites for instant messaging or social networking
    4. use of file sharing software
    5. accidentally corrupting or destroying other people's data without notifying staff
    6. accidentally accessing offensive material without notifying staff

    Sanctions could include: referral to class teacher or tutor; loss of internet access for a period of time; removal of mobile phone until the end of the day; contacting parents.
4. Student Category D infringements. These are typically low-level breaches of acceptable use agreements such as:
    1. use of non-educational sites during lesson
    2. unauthorised use of email or mobile phones
    3. unauthorised use of prohibited sites for instant messaging or social networking

    Sanctions could include referral to the class teacher or tutor where infringement is persistent.
5. Staff Category A infringements. These involve deliberate actions that undermine safety on the school IT system and activities that call into question the person's suitability to work with children. They represent gross misconduct that would require a strong response and possible referral to other agencies..
    1. serious misuse of or deliberate damage to any school computer hardware or software, for example deleting files, downloading unsuitable applications
    2. any deliberate attempt to breach data protection or computer security rules, for example hacking
    3. deliberately accessing, downloading or disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
    4. receipt or transmission of material that infringes copyrights or is in breach of the Data Protection Act
    5. bringing the school name into disrepute

    Possible sanctions include: referral to the Principal; removal of equipment; referral to police; suspension pending investigation; disciplinary action in line with school policies
6. Staff Category B infringements. These are minor breaches of the school's acceptable use policy which amount to misconduct and will be dealt with internally by the Principal
    1. excessive use of internet for personal activities not connected to professional development
    2. any behaviour on the internet that compromises the staff member's professional standing in the school and community, for example inappropriate comments about the school, staff or students or inappropriate material published on social networking sites
    3. sharing or disclosing passwords to others or using other user's passwords
    4. breaching copyright or licence by installing unlicensed software

    Possible sanctions include referral to the Principal who will issue a warning.

Revision Control Table	
Drawn up by	Admin team
Date	22/9/17 Approved by DS
Review schedule	Annual
Reviewed	1/6/18 by DS; 1/6/19 by DS; 01/06/20 by DS (tidying and editing); 10/9/21 by DS; 10/10/22 by DS; 15/09/23 by DS; 20/11/24 by DS (minor edits)
Next review	01/12/25