The Sir John Colfox Academy

Acceptable Use of ICT Policy

Headteacher:	**Adam Shelley**
Policy Written by	**The Sir John Colfox Academy**
Policy Reviewed	**September 2020**
Ratified by Board of Governors	**October 2020**
Date for Review	**October 2023**

Signature of Chair _____

Acceptable Use of ICT Policy

Rationale

Digital technologies are integral to the lives of young people both within school and outside of school. The internet and other technologies are powerful tools which open up new opportunities. Electronic communication promotes effective teaching and learning through the multiplicity of digital and information applications. All young people have an entitlement to access such technologies, to enhance motivation and engagement and thus facilitate continued improvements in standards across all curriculum areas.

The requirement to ensure that young people are able to use technologies appropriately and safely should be addressed as part of the wider duty of care to which all those who work in schools are bound. This e-safety policy should ensure safe and appropriate use. The implementation of this strategy involves all stakeholders in the school community.

At the Sir John Colfox Academy students in years 7-11 are not permitted to use their personal handheld devices e.g. mobile phones in school. The school recognises the impact that handheld technology can have on learning and iPads, iPods, Chromebooks, and other school owned technology may be used to help learning. However, for safeguarding reasons, students are asked to have their personal devices switched off when in school. Sixth form students are permitted to use their devices and have wireless access when in school. Their use is monitored by the IMPERO system.

Purpose

This policy addresses the potential risks associated with digital technology:

- Access to illegal, harmful or inappropriate images
- Unauthorised access to, or loss of, or inappropriate sharing of personal information
- Access to harmful websites, for example those devoted to weapons production, how to take one's own life or promoting high risk behaviours
- The risk of being subject to grooming via the internet, and possibly meeting high risk individuals offline
- The sharing and/or distribution of personal images without the individual's consent or knowledge
- Inappropriate communication with others including strangers
- Cyber bullying
- Access to unsuitable video/internet games
- The inability to evaluate the accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of files
- The potential for excessive/obsessive use

Guidelines

Technical Requirements

1. The Sir John Colfox automatically receives the benefits of the SWGfL managed filtering service. This is managed by the Network Manager in order to ensure that the school meets the e-safety technical requirement outline in the SWGfL Security Policy.
2. The filtering of internet content provides an important means of preventing users from accessing material that is illegal or inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, so

education and training and monitoring of activity are required to reduce, as far as possible, the risks to students.

3. Impero software is used in school to monitor ICT activity, internet use and online safety within the classroom.

Education and Training

- All users of the school network receive e-safety training so that they recognise and avoid e-safety risks, build their resilience and understand their responsibilities. This is monitored and overseen by the E-safety officer
- The school E-Safety Officer attends regular e-safety training and provides training and advice for members of students, staff and governors.
- Students receive formal e-safety training through ICT lessons, PSHE, assemblies; E-safety messages are reinforced through ICT across the curriculum.
- The education for students is regularly reviewed to keep pace with new issues that young people might face when 'online'. This includes guidance on Sexting and the dangers and warning signs of child sexual exploitation and what to do when there are any concerns.
- The students also receive guidance on the dangers of radicalisation in an online environment and how to sport warning signs and what to do if they are concerned.
- The school provides information and awareness to parents and carers letters, newsletters and the website.

Acceptable Use Policies

The school tries to provide all users with good access to ICT to enhance their work, to enhance learning opportunities and, in return, expect students, staff and volunteers to agree to be responsible users. All users are provided with a username and strong password by the ICT system Administrators (which they must not share with others) when they have signed the appropriate Acceptable Use Policy. (Appendix 1)

The Acceptable Use Policy is intended to ensure that:

- all users will be responsible and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their online behaviour
- parent and carers understand that digital images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.
- parents and carers agree that if they take digital or video images at, or of, school events, which include images of children other than their own, that they will abide by the school guidelines in the use of these images.

Use of Photographic and Video Images

- Students and Staff may take and use digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Images must only be taken on school equipment.
- Written permission from parents or carers and students must be obtained before photographs of students are published on the school website or used for publicity that reasonably celebrates success and promotes the work of the school. Permission is sought using the Minerva Learning Trust Data Consent form and a list of students for whom there is no permission is held by the school on Bromcom.

Communications

- Students are provided with individual school email addresses for educational use and must immediately report, to a teacher if they receive any email that makes them feel uncomfortable, is suspicious, offensive, threatening or bullying in nature and must not respond to any such email. This information must be passed to the school E-Safety Officer
- Any communication between staff and students or parents / carers (email, VLE, Twitter, Facebook etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems or professional accounts. Personal email addresses, text messaging or chat and social networking programmes must not be used for these communications.
- Students and staff should not engage in social conversations with each other via email, text or social networking sites sites such as Facebook or Twitter
- Users are made aware, through training, that email and other communications may be monitored

Responding to incidents of misuse

- All members of the school community are expected to be responsible users of ICT; however, there may be times when infringements of the policy could take place, through careless, irresponsible or, very rarely, deliberate misuse.
- There is no tolerance of cyber-bullying.
- If members of staff suspect that misuse might have taken place, but that the misuse is not illegal it must be reported to the school Network Manager or E-Safety Officer as soon as possible and will be dealt with through normal behaviour / disciplinary procedures.
- If any apparent or actual misuse appears to involve illegal activity the school follows the SWGfL guidance and flow chart (see Appendix 2)

Monitoring and evaluation

- The IT team monitors the impact of the policy using the SWGFL, Impero Software and internal logging of incidents. Any suspicious or inappropriate activity is reported to the school Senior Leader responsible for E-safety
- This policy is reviewed annually by the school Senior Leader responsible for E-safety, working with the E-safety Officer, the Network Manager and the Senior Leader responsible for the IT infrastructure

Appendix 1

Students

The Sir John Colfox Student ICT Acceptable Use Agreement

The school will ensure that you have good access to ICT to enhance your learning and you will agree in return to be a responsible user.

Student Signature

I have read and understand the policy below and agree to use the school ICT systems appropriately. I understand that careless or malicious damage may not be covered by the school insurance.

Student name: ..... Signature ..... Date .....

Parent Signature

I/we have read and understand the policy below and agree to support our child in the safe and appropriate use of their device. I/we commit to monitor how my/our child uses and cares for their devices and understand that careless or malicious damage may not be covered by the school insurance. I will ensure that my child keeps the device in the case provided at all times.

Parent name: ..... Signature ..... Date .....

Rationale

This Acceptable Use Policy is intended to ensure

• that students stay safe while using the internet and other communications technologies

• that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk

• that student's devices are cared for and used in an appropriate fashion

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that I act responsibly at all times.

• I understand that the school will monitor my use of the ICT systems, email and other digital communications.

• I understand that the rules set out here apply to all ICT provided by the school (iPads, netbooks, laptops, email, VLE etc) out of school as well as in school

• I understand that the school ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use while in lessons.

Continued....

• I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.

• I will immediately report any illegal or harmful material or incident I become aware of, to a member of staff

• I will not access, copy, remove or alter any other user's files or data

• I will communicate with others in a reasonable manner, I will not use aggressive or bad language and I appreciate that others may have different opinions to my own.

• I will ensure that if I take images/videos of others I will only do this if they know about it and have agreed.

• When I use my device in school, I will follow the rules in the same way as if I was using school equipment.

• I will not upload, download or view anything which is illegal such as pornography or racist materials or anything which will cause upset to others.

• I will not use any programmes or software that might allow me to bypass the filtering / or any IT security systems.

• I will not make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

• I will not install or attempt to install programmes of any type on a school PC, or install programmes on a computer, nor will I try to alter PC settings.

• I will not modify my device and realise that if I do that will invalidate the warranty and insurance

• I will not disable or cause any damage to school equipment, or the equipment belonging to others.

• I will immediately report any damage or faults involving equipment or software, however this may have happened.

• I will ensure that I have permission to use the original work of others in my own work and that I acknowledge this.

• Where work is protected by copyright, I will not download or distribute copies (including music and videos).

• I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school.

• I understand that if do not follow this Acceptable Use Policy Agreement, I could be subject to sanctions which could include exclusion from school and the involvement of the police.

Staff

The Sir John Colfox Staff ICT Acceptable Use Agreement

User Signature

I have read and understand the policy below and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff Name ..... Signature ……..……
Date ……

iPad serial number .....

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for students learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg tablets, , laptops, email, VLE etc) out of school

- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person. I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only communicate with students/pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held/external devices (PDAs/laptops/mobile phones/USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will ensure all personal electronic devices are PAT tested prior to using them in school
- I will not use personal email addresses on the school ICT systems
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering /security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.

- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School /LA Personal Data Policy. Where personal data is transferred outside the secure school network, it must be encrypted.
- I understand that data protection policy requires that any staff or student/pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

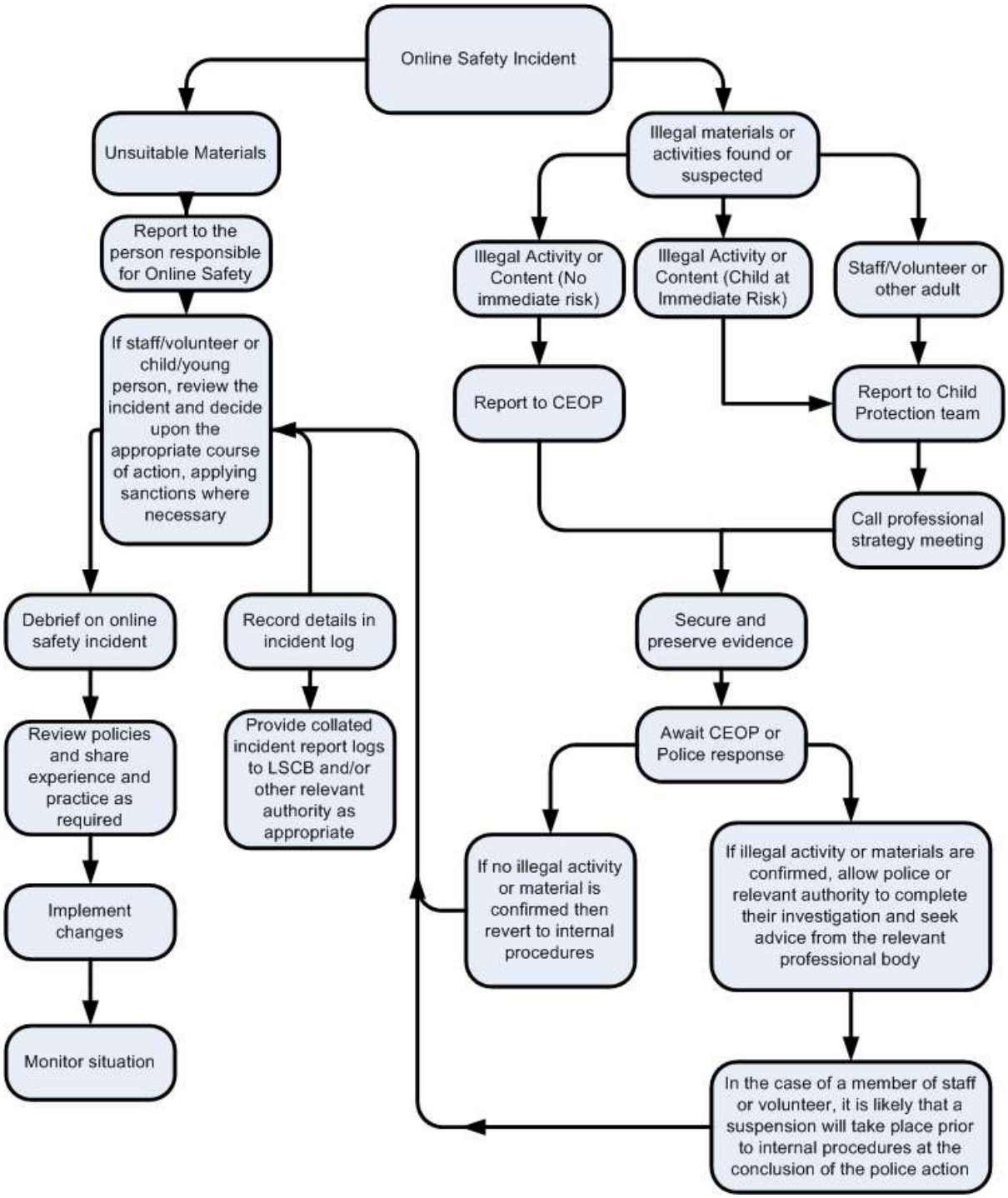
When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and/or the Local Authority and in the event of illegal activities the involvement of the police.
- Linked Policies
  - Data Protection
  - Mobile Technologies
  - Staff Code of Conduct
  - Social Media Policy

Appendix 2.
Responding to incidents of misuse – flow chart


Online Safety Incident
Unsuitable Materials
Illegal materials or activities found or suspected
Report to the person responsible for Online Safety
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Debrief on online safety incident
Record details in incident log
Secure and preserve evidence
Review policies and share experience and practice as required
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Await CEOP or Police response
Implement changes
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
Monitor situation
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action