ON-LINE SAFETY POLICY

Contents

5.5 Students use of social media

- Safe and responsible use of social media sites will be outlined for pupils/students and their parents as part of the school's AUP.
- Personal publishing on social media sites will be taught to pupils/students as part of an embedded and progressive education approach via age appropriate sites that have been risk assessed and approved as suitable for educational purposes.
- Pupils/students will be advised to consider the risks of sharing personal details of any kind on social media sites that may identify them and / or their location. Examples would include real/full name, address, mobile or landline phone numbers, school attended, Instant messenger contact details, email addresses, full names of friends/family, specific interests and clubs, etc.
- Pupils/students will be advised not to meet any online friends without a parent/carer or other responsible adult's permission and only when they can be present.
- Pupils/students will be advised on appropriate security on social media sites and will be encouraged to use safe and passwords, deny access to unknown individuals and be supported in learning how to block and report unwanted communications.
- Pupils/students will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private/protected.
- Any official social media activity involving pupils/students will be moderated by the School where possible.
- The School is aware that many popular social media sites state that they are not for pupils/students under the age of 13, therefore the School will not create accounts within school specifically for children under this age.
- Any concerns regarding pupils'/students' use of social networking, social media and personal publishing sites, both at home and at School, will be dealt with in accordance with existing School policies including Anti-Bullying and Behaviour.
- Any concerns regarding pupils'/students' use of social networking, social media and personal publishing sites, both at home and at School, will be raised with parents/carers, particularly when concerning any underage use of social media sites.

6.0 Use of Personal Devices and Mobile Phones

6.1 Rationale regarding personal devices and mobile phones

- The widespread ownership of mobile phones and a range of other personal devices among pupils/students and adults will require all members of the Trust community to take steps to ensure that mobile phones and personal devices are used responsibly within and outside of School.
- The use of mobile phones and other personal devices by pupils/students and adults within school will be decided by each school and is covered in appropriate policies including the Mobile Phone Policy.

6.2 Expectations for safe use of personal devices and mobile phones

- All use of personal devices and mobile phones will take place in accordance with the law and other appropriate School policies
- Electronic devices of all kinds that are brought in on site are the responsibility of the user at all times. The School accepts no responsibility for the loss, theft or damage of such items. Nor will the School accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community and any breaches will be dealt with as part of the Behaviour for Learning policy and Anti-Bullying policy.
- Members of staff will be issued with a work phone number and email address where contact with pupils/students or parents/carers is required.
- All members of the Trust community will be advised to take steps to protect their mobile phones or devices from loss, theft or damage.
- All members of the Trust community will be advised to use passwords/PINs to ensure that unauthorised calls or actions cannot be made on their phones or devices if they are lost or stolen. Passwords and PINs should be kept confidential. Mobile phones and personal devices should not be shared.
- All members of the Trust community will be advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the School's policies.
- School mobile phones and devices must always be used in accordance with the school's AUP.
- School mobile phones and devices used for communication with parents and students must be suitably protected via a passcode/password/PIN and must only be accessed and used by members of staff.

6.3 Students use of personal devices and mobile phones

- Pupils/students will be educated regarding the safe and appropriate use of personal devices and mobile phones.
- All use of mobile phones and personal devices by pupils/students will take place in accordance with the Mobile Phone and Electronic Device Policy.
- Pupils'/students' personal mobile phones and personal devices will be kept in a secure place, switched off and kept out of sight during school hours.
- If a pupil/student needs to contact his/her parents/carers they will be allowed to use a school phone outside of lesson time.
- Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Pupils/students should protect their phone numbers by only giving them to trusted friends and family members.
- Pupils/students will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

- Mobile phones and personal devices must not be taken into examinations/tests. Pupils/students found in possession of a mobile phone or personal device during an exam/test will be reported to the appropriate examining body. This may result in the pupil's/student's withdrawal from either that examination/test or all examinations/tests.
- School staff may confiscate a pupil's/student's mobile phone or device if they believe it is being used to contravene the School's Behaviour or Anti-Bullying Policy or could contain youth produced sexual imagery (sexting). The phone or device may be searched by a member of the SLT. Searches of mobile phone or personal devices will only be carried out in accordance with the DfE guidance which can be found at the following link: https://www.gov.uk/government/publications/searching-screening-and-confiscation
- If there is suspicion that material on a pupil's/student's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence then the device will be handed over to the police for further investigation.

6.4 Staff use of personal devices and mobile phones

- Members of staff are not permitted to use their own personal contact details for contacting pupils/students and their families within or outside of the setting in a professional capacity. Any pre-existing relationships which could compromise this will be discussed with their line manager.
- Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of children and will only use work-provided equipment for this purpose.
- Bluetooth or other forms of communication on personal devices should be "hidden" or switched off during lesson times.
- Personal mobile phones or devices will not be used by teaching staff during teaching periods unless permission has been given by a member of the Leadership Team in emergency circumstances
- Staff will ensure that any content bought on site via mobile phones and personal devices are compatible with their professional role and expectations.
- If a member of staff breaches this policy then disciplinary action may be taken.
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence then the police will be contacted.
- Any allegations against members of staff involving personal use of mobile phone or devices will be responded to following the Allegations Management Policy.

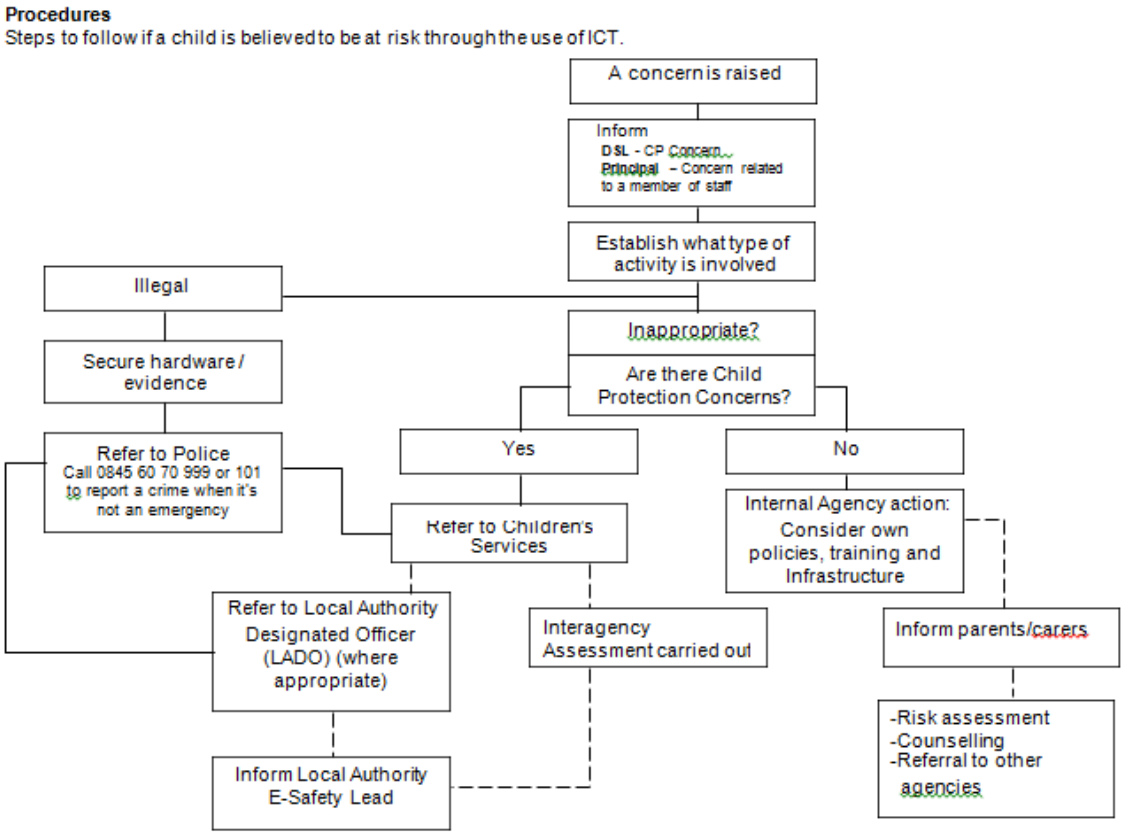
6.5 Visitors use of personal devices and mobile phones

- Parents/carers and visitors must use mobile phones and personal devices in accordance with the school's Acceptable Use Policy.
- Use of mobile phones or personal devices by visitors and parents/carers to take photos or videos is not allowed on school site.

- Each school will ensure appropriate signage and information is displayed and provided to inform visitors of expectations of use.
- Staff will be expected to challenge concerns when safe and appropriate and will always inform the DSL of any breaches of use by visitors.

Appendix A:

Guidance on what to do if a concern is raised following an online safety incident:



Appendix B:

Responding to concerns regarding radicalisation and extremism online

- The School will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the internet in schools and that suitable filtering is in place which takes into account the needs of pupils/students. (Refer to item 4.3 filtering and monitoring.)
- When concerns are noted by staff that a child may be at risk of radicalisation online then the Designated Safeguarding Lead (DSL) will be informed immediately and action will be taken in line with the safeguarding policy.
- Online hate content directed towards or posted by specific members of the community will be responded to in line with existing school policies, including Anti-Bullying, Behaviour, etc. If the School is unclear if a criminal offence has been committed then the Designated Safeguarding Lead will obtain advice immediately via the LA Safeguarding Team and/or the Police.

Appendix C

Information & Organisations

CEOP - The Child Exploitation and Online Protection Centre is part of UK police and is dedicated to protecting children from sexual abuse wherever they may be. That means building intelligence around the risks, tracking and bringing offenders to account either directly or with local and international forces and working with children and parents to deliver our unique Think U Know educational programme. http://ceop.police.uk
Childnet International's mission is to work in partnership with others around the world to help make the Internet a great and safe place for children. Childnet works in 3 main areas of Access, Awareness, Protection & Policy. http://www.childnet.com
DfE - The Department for Education is responsible for education and children's services. http://www.education.gov.uk
IWF – The Internet Watch Foundation was established in 1996 by the UK internet industry to provide the UK internet 'Hotline' for the public and IT professionals to report potentially illegal online content within their remit and to be the 'notice and take-down' body for this content. IWF works in partnership with the online industry, law enforcement, government, the education sector, charities, international partners and the public to minimise the availability of this content, specifically, child sexual abuse content hosted anywhere in the world and criminally obscene and incitement to racial hatred content hosted in the UK. http://www.iwf.org.uk
Know IT All for Parents contains advice for parents and carers, and a special section for children and young people. http://www.childnet.com/kia/parents/
Local Safeguarding Children Board http://www.bathnes.gov.uk/services/children-young-people-and-families/child-protection/local-safeguarding-children-board
Report Abuse http://ceop.police.uk/safety-centre
UK Safer Internet Centre (UKSIC) - The UK Safer Internet Centre is co-funded by the European Commission and brought to you by a partnership of three leading organisations, Childnet International, the South West Grid for Learning and the Internet Watch Foundation. The UK Safer Internet Centre has three main functions: An Awareness Centre, a Helpline and a Hotline. http://www.saferinternet.org.uk

Appendix D – Staff Acceptable Use 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 access to the internet and digital technologies 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 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 technology in their everyday work.

The School will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils'/*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's systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that pupils/students receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the School will monitor my use of the School's digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of School.
- I understand that the School's digital technology 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 understand that I should not write down or store a password where it is possible that someone may steal it.
- 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 use social networking sites in School in accordance with the School's policies.
- I will only communicate with pupils / students and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line 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 mobile devices (laptops / tablets / 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 not use personal email addresses on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (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 / academy 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 / academy 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 Data Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or pupil / student 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 the School:

- I understand that this Acceptable Use Policy applies not only to my work and use of School digital technology equipment in school, but also applies to my use of School systems and equipment off the premises and my use of personal equipment on the premises 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 / Directors and / or the Local Authority and in the event of illegal activities the involvement of the Police.

Appendix E – Pupil/Student Acceptable Use Policy

ICT Acceptable Use Policy for Students

School laptops and iPads, School network access, internet use

Be Responsible

I will:

- ✓ Use electronic devices, the internet and the School network for educational purposes as directed by my teacher
- ✓ Use only my own accounts
- ✓ Securely log off at the end of each session

Be Respectful

I will:

- ✓ Communicate online in a respectful manner
- ✓ Treat school equipment with care
- ✓ Respect the work and privacy of others

Be Safe

I will:

- ✓ Keep my password and login information private
- ✓ Tell an adult if I read or see something on the internet that makes me feel uncomfortable
- ✓ Refrain from sharing any personal information on the internet

I understand that the use of technology is a privilege, not a right and inappropriate use will result in a cancelation of these privileges and may also include disciplinary action.