Woodrush High School

An Academy for Students Aged 11-18

ICT and E-Safety Policy

Policy author / reviewer	J Barber
Responsible LGB committee	Teaching and Learning
Date ratified	June 2021
Status	Statutory
Date of next review	Every 3 years

ICT and the internet have become integral to teaching and learning within schools; providing children, young people and staff with opportunities to improve understanding, access online resources and communicate with the world all at the touch of a button.

At present, the internet based technologies used extensively by young people in both home and school environments include:

- Websites
- Music Streaming Services, including Youtube, Spotify
- Social Media, including Instagram, SnapChat, Facebook and Twitter
- Online gaming
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Email, Instant Messaging and Chat Rooms
- Voice

And these are accessed via:

- Web enabled mobile/smart phones
- Tablets
- Games consoles
- PC
- SMART technology devices

Whilst this technology has many benefits for our school community, we recognise that clear procedures for appropriate use and education for staff and students about online behaviours, age restrictions and potential risks is crucial.

At Woodrush High School we are committed to ensuring that students are kept safe when using the Internet and other new technologies without limiting their opportunities for creativity and innovation.

Both this policy and the Acceptable Use Agreements (for all staff, governors, visitors and students) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by students and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

1. Use of school equipment.

In general, members of the School may use those computing facilities that they are authorised to access providing that the use is related to their job (for staff) or their course (for students). Modest use for private non-academic purposes is usually acceptable, however users must recognise that such use must not adversely affect the operation of the School.

1.1 All users of the school ICT equipment are responsible for their activity and record is kept of ICT equipment issued to staff as part of the school's inventory.

1.2 All ICT equipment is to be kept physically secure both in school and or out of school.

1.3 No user is to attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990

1.4 On termination of employment, resignation or transfer all ICT equipment must be returned to the school.

1.5 All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)

1.6 School systems and networks must not be used for:

- Copyright infringement or Plagiarism
- The sending of messages which are racially, sexually or personally abusive
- The corruption or destruction of other users data
- The initiation or spread of electronic chain mail or SPAM
- Any activity which is wasteful of resources such as playing of computer games.
- Defamation or libellous attacks on persons
- Any activity which may reflect adversely upon the School

1.7 Virus scanning software has been installed on all networked PC systems in the School, however, all users must take the necessary steps to protect School systems from viruses by adhering to the following rules:

- Any software programs must not be installed or executed without the prior approval of IT Dept., and in particular:
- Computer Games.
- Public domain software, shareware or peer to peer software
- Any unauthorised program attached to an email message
- Any programs obtained from the Internet
- The following categories of computer media must always be scanned for viruses:
  - Any originating from outside the School
  - Any used on a home computer
  - Removable storage devices such as CD's, DVD's or USB flash memory

2. Data security

2.1 The school gives relevant staff access to its Management Information System (currently Arbor), with a unique username and password and it is the responsibility of everyone to keep passwords secure and difficult to guess.

2.2 If any staff or student believes their password has been compromised they must inform the E safety co-ordinator immediately and get a new, secure password.

2.3 Staff must keep all school related data secure. This includes all personal, sensitive, confidential or classified data

2.4 Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight

2.5 Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times

2.6 It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed.

2.7 Personal, sensitive, confidential or classified data can only be stored on a portable storage device if it is encrypted.

2.8 Remote access to school network drives must only be done through a computer or device with an appropriate level of security and every care should be taken to protect school information and data. You cannot connect a VPN to the school on a computer that doesn't not have the school's managed anti virus software installed.

2.9 Personal, sensitive, confidential or classified data should not normally be transferred via email. If this is unavoidable the following steps should be taken

- The recipient address should be check and confirmed
- The information should be **attached** to the emailed in an **encrypted** document
- The encryption password should be given to the recipient by a method other than email
- A request for confirmation of safe receipt must be sent
- Microsoft 365's built in encryption must be turned activated on the email

3. Use of email

3.1 The school gives all staff their own e-mail account to use for all school business as a work based tool This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed

3.2 Information must not be transmitted internally or externally which is beyond the bounds of generally accepted standards, values and ethics. This includes, for example, material which could be considered offensive or discriminatory; pornographic or obscene, defamatory or libellous or any other material which is otherwise abusive or contains illegal content prohibited by law or regulation or which brings the School into disrepute or which contravenes School policies.

3.3 All material contained on the email system belongs to the School and staff should not consider messages produced/received by them on School equipment/software (owned or licensed) to be secure. The confidentiality of email cannot be assured and staff should be aware of the possibilities of intended or accidental onward transmission to others beyond the original addressee(s). Furthermore, it is possible to retrieve deleted emails from back-up files intended to assure system integrity and reliability.

3.4 It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business

3.5 Staff transferring or receiving files or attachments from external sources should note that the School system automatically checks downloaded material for viruses. However, in the event that a virus is suspected, the file or attachment must not be opened and the matter must be reported to the IT department immediately for inspection and action

3.6 Under no circumstances should staff contact students, parents or conduct any school business using personal e-mail addresses

3.7 Reasonable personal use of the email system is permitted, subject to the approval of Headteacher and the constraints and conditions set out in this Policy and the Regulations. The Headteacher may define the level of use, as appropriate, in their areas. Personal use must not interfere with the operation of School services, involve cost implications for the School or take precedence over the user's job accountabilities.

3.8 Authorisation to use the School PCs at home or School software on home PCs will be withdrawn on the termination of the employee's contract of employment and computer records of emails sent and received will be destroyed after a suitable period of time by IT Management.

3.9 Where it is considered that there has been a breach in the use of the email system, any intercepted emails will be referred to the Network Manager for examination of the contents and this should be referred to the Headteacher

3.10 All students will be provided with a school email account. Student e-mail users are expected to adhere to the generally accepted rules of internet etiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.

3.11 The school adheres to Microsoft default retention policy. All emails in deleted items will be deleted and unrecoverable after 30 days.

4. Internet access

4.1 The School provides access to the Internet and its resources for the purposes of teaching, research and other school business. Justifiable reasonable personal use of the Internet is permitted, according to constraints and conditions set out in the Policy and Regulations. Personal use must not interfere with the operation of School duties, involve cost implications for the School or take precedence over the user's work accountabilities.

4.2 Internet software may only be installed by or with the agreement of Network Manager. No unapproved or downloaded software may be used unless the integrity, continuity and full support of the product can be guaranteed. Software patches or updates may only be downloaded from officially supported vendors, subject to IT department approval and ensuring strict adherence to the vendor's security and usage guidelines.

4.3 The School reserves the right to block access to any Internet resource. Academic access to blocked sites may be arranged on application via the Network Manager.

4.4 Users must not access, retrieve, print or distribute text or graphical information that is beyond the bounds of generally accepted standards, values and ethics. This includes, for example, material which could be considered offensive or discriminatory, pornographic or otherwise obscene; defamatory or libellous or any other material which contains illegal content prohibited by law or regulation.

4.5 To protect School systems from imported viruses, downloading or exchanging screensavers, games, entertainment software or other inappropriate files (for example, video or audio materials for personal use), playing games against opponents or gambling over the internet is not permitted. Where such use is suggested for training or development purposes, it must have the specific agreement of the Headteacher and Network Manager.

4.6 Users may not conduct any form of "hacking" or use malicious code to penetrate or attempt to penetrate other computers or to deliberately release viruses or other harmful programs within either the School network or the internet or bypass security features.

5. E-safety

ICT and online resources are increasingly used across the curriculum. We believe it is essential for E-safety guidance to be given to the students on a regular and meaningful basis. E-safety is embedded within our curriculum and we continually look for new opportunities to promote E-safety. E-safety encompasses internet technologies and electronic communications such as mobile phone and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences. The named E-safety co-ordinator in this school is JYB who has been designated this role as a member of the senior leadership team. This part of the policy, supported by the school's acceptable use agreements for staff, governors, visitors and students, is to protect the interests and safety of the whole school community.

5.1 E-safety in embedded in the curriculum so that students learn to be in control of their own safety online - The school has a framework for teaching internet skills in ICT/ ASPIRE lessons can be obtained from the E Safety Co-ordinator

5.2 Internet activity is monitored in school and virus protection is installed and updated regularly.

5.3 The school internet is provided by a safe and secure source**.**

5.4 Students will be taught what internet use is acceptable and what is not as well as being educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

5.5 E-safety guidelines will be regularly highlight students through displays in ICT rooms, information in planners and assemblies (as well as curriculum based lessons). The school will also participate in Safer Internet Day each year.

5.6 Images of students will not be used around school, on the school website or for publicity purposes without parental permission as set out in the school's Photos and Images Policy.

5.7 Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

5.8 Students will be advised never to give out personal details of any kind which may identify them, their friends or their location.

5.9 Students should not place personal photos on any social network space without considering how the photo could be used now or in the future.

5.10 Students should be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications. Students should only invite known friends and deny access to others.

5.11 Cyberbullying takes different forms: threats and intimidation, harassment or 'cyber-stalking' (e.g. repeatedly sending unwanted texts or instant messages), vilification/defamation; exclusion or peer rejection, impersonation, unauthorised publication of private information or images (including what are sometimes misleadingly referred to as 'happy slapping' images), and manipulation. Cyberbullying, like all bullying, is taken very seriously and is never acceptable.

5.12 It is not acceptable to write comments, make or upload images or videos of any individual without their express written permission. This includes members of staff, visitors, the general public and any other student(s) of this or any other school.

5.13 The school will record and monitor incidents of cyberbullying in the same way as all other forms of bullying and the same sanctions will apply. Please see the school behaviour policy for further information.

6. Incident reporting

6.1 Where it is considered that there has been a breach in the use of the School email / Internet system the following Disciplinary Procedures will be put into practice.

Staff

The Network Manager will notify a member of the Senior Leadership that he considers that there has been a breach in the use of the School computer system.

The Headteacher will consider the facts presented and if it is considered that there has possibly been inappropriate use, the Network Manager will be instructed to disable the user's access until further notice. Depending on the particular case, the Headteacher may follow other policies e.g Disciplinary, Safeguarding etc. which require their own processes/investigations

Students

The Network Manager will notify a member of the Senior Leadership or appropriate Head of Year that he considers that there has been a breach in the use of the School's computer system.

The staff concerned will consider the facts presented and if it is considered that there has been inappropriate use the Network Manager will be instructed to disable the Student's access until further notice.

6.2 All incidents regarding e-safety will be dealt with using E Safety Incident Flow Chart. *Appendix 4*

6.3 All E-safety incidents will be logged by the staff involved on Arbor and the E Safety Coordinator will be kept informed. In incidences of cyber bullying they may also be recorded elsewhere.

7. Other technologies

7.1 Restricted use of mobile phones is allowed within school as outlined in the schools' Mobile phone policy. *Appendix 5*

7.2 Currently students are not permitted to bring in other mobile electronic devices. Should they choose to do so the school will not be held liable for loss, theft or damage.

7.3 All activity on other new technology devices will be monitored in accordance with school policy.

8. Social media

Facebook, Twitter and other forms of social media are increasingly becoming an important part of our daily lives.

8.1 Staff are not permitted to access their personal social media accounts using school equipment from school during school hours

8.2 Students are not permitted to access their social media accounts whilst at school

8.3 Staff, governors, students, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others

8.4 Staff, governors, students, parents and carers are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever

8.5 Staff, governors, students, parents and carers are aware that their online behaviour should, at all times, be compatible with UK law

8.6 Any social media account that is set up by a member of staff as part of their teaching activities or to keep parents or students aware of school activities must be approved by SLT and only be used in a way that is not incompatible with their role in the school and does not bring the school into disrepute. Twitter use for teaching and learning purposes must adhere to the guidelines set out in the Twitter Use in School Policy A*ppendix 6*

8.7 Staff are advised to read guidance from their professional association regarding conduct and privacy settings on social networking sites.

9. Monitoring

9.1 Authorised ICT technicians and management may inspect any ICT equipment owned or leased by the school at any time without prior notice. Website usage and email messages are regularly monitored and the School reserves the right to intercept communications for inspection (in line with the Regulation of Investigatory Powers Act, The Data Protection Act and the Freedom of Information Act) should an incident occur where inappropriate use of the facilities is suspected.

9.2 Any violation of the provisions (for example, downloading pornographic material, sending offensive messages, harassment, discrimination, spamming or hacking) may result in action up to and including dismissal under the School's Disciplinary Procedures. In the event that legislative requirements are breached, then the perpetrator(s) will also be subject to other action.

10. Roles and responsibilities

10.1 SLT are responsible for the administration of this Policy and the regulations for the use of School computer systems, networks and facilities. Overall accountability for Data Protection within the School rests with the clerk to the Governors, although operational responsibility for staff data is held by the Head's PA and for Student records is held by Arbor which is maintained by the data manager. However, all Line Managers are responsible for the conduct and performance of their staff, their usage of school facilities and equipment and their adherence to the contents of this Policy and the Regulations. The E Safety Coordinator is responsible for overseeing E-safety within the school.

10.2 Every School computer user agrees to abide by the terms and conditions set out in this Policy and the Regulations. Every user must accept responsibility for the protection of electronically accessed information against loss, disclosure or misuse.

10.3 All users must be aware of their responsibilities and obligations to others under the terms of the Data Protection legislation. Particular care must be exercised in respect of data held about other people both inside and outside the School for operational, research or any personal purposes.

10.4 This policy is agreed by SLT, approved by governor and reviewed on a yearly basis (or sooner if necessary).

Appendix 1 – Student Acceptable Use Policy

- I will only use ICT systems in school, including the internet, Office 365, e-mail, digital video and mobile technologies for educational purposes
- I will not download or install software on school technologies.
- I will only log onto the school network other systems and resources with my own user name and password.
- I will not permit others to perform any actions logged into my user account.
- I will follow the school ICT security system notifications, not reveal my passwords to anyone and change my password regularly.
- I will make sure that all ICT communications with students, teachers or others are responsible and sensible
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet up with someone outside of the school unless this is part of a school project approved by my teacher.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, students or others distress or bring anyone into disrepute.
- I will support the School's approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I will respect the privacy and ownership of others' work online at all times.
- I will not attempt to bypass the internet filtering system.
- I will conserve resources by only printing what is necessary for my work.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/ carer may be contacted

Appendix 2 – Staff/Visitor Acceptable Use Policy ICT

This includes data and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the school E-safety coordinator or school network manager.

- I will only use the school's email / Internet / Microsoft 365 and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with students and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, to students.
- I will only use Microsoft 365, the approved, secure e-mail system for any school business.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted.
- I will not install any software without permission of the Network Manager.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of students and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/carer, member of staff or Headteacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher. I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute including activity on social networking sites.
- I will support and promote the school's e-Safety and Data Security policies and help students to be safe and responsible in their use of ICT and related technologies.

User Signature

I agree to follow this Acceptable Use Policy and to support the safe and secure use of ICT throughout the school.

Signature ……. Date ……..

Full Name ……(printed)

Appendix 3 – Relevant Legislation

The major UK legislation applicable to computer and network use is referred to below. This document can only offer very general guidelines on the legislation. For further information please contact the Network Manager who will be able to suggest sources of more detailed information.

The Computer Misuse Act (1990)
It is an offence to access, or try to access, any computer system or material for which authorisation has not been given. Any attempt to bypass security controls on a computing system is also an offence, as is facilitating unauthorised access, by, for example, the disclosure of a user id or password.

The Copyright, Design and Patents Act (1988)
Almost all computer software in use in the School is protected under this Act, which gives the owners of the copyright the exclusive right to copy a protected work. It is therefore illegal to copy any software without the copyright owner's permission. Software may only be used for the purposes defined in the licensing agreement, and on the computer systems to which that agreement applies. Terms and conditions of license agreements vary considerably from product to product. Users must also ensure they have the permission of the copyright holder to publish material on web pages under their control.

The Data Protection Act (1998)
The Data Protection Act relates to the automatic processing of personal data, that is information relating to a living person, and is applicable to computerised and also some manual systems. The Act gives individuals certain legal rights regarding information held about them by others, and sets requirements for organisations to meet before personal data can legally be processed.

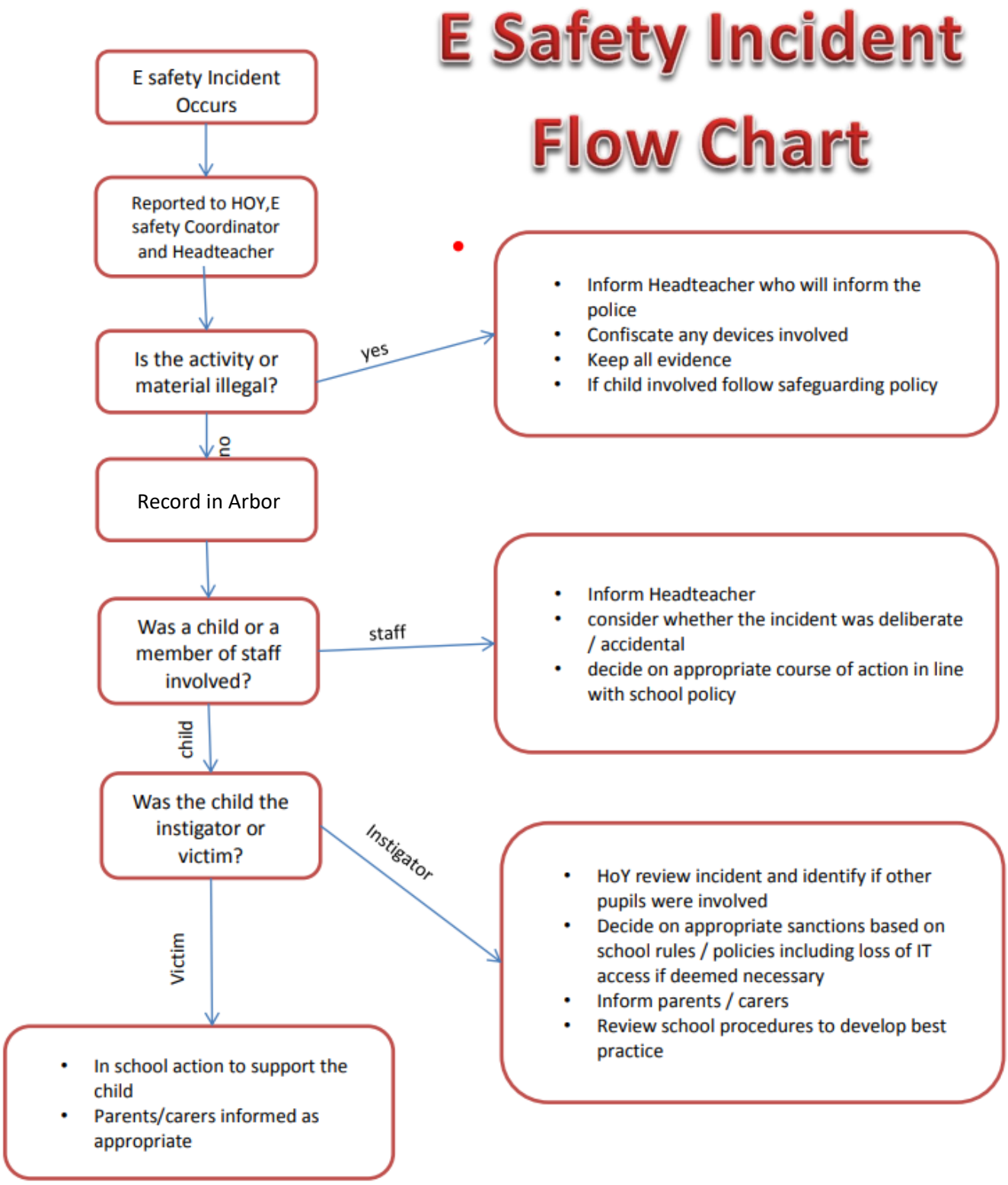
The Criminal Justice and Public Order Act (1994)
This Act extends the scope of the Obscene Publications Act 1959 to make the storage and electronic transmission of obscene material arrestable offences.

The Protection of Children Act (1978)
Relating to images of children transmitted, sourced or created using computers

The Regulation of Investigatory Powers Act (2000)
This Act repeals prior legislation in the area of interception of communications Act (1985) and implements article (5) of the EU Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the communications sector.

UK General Data Protection Regulation (UK GDPR)

Appendix 4 – E Safety Incident Flow Chart



Appendix 5 – Mobile Phone Acceptable Use Policy

1. Purpose

1.1. The widespread ownership of mobile phones among young people requires that school administrators, teachers, support staff, students, parents and carers take steps to ensure that mobile phones are used responsibly at school. This Acceptable Use Policy is designed to ensure that potential issues involving mobile phones can be clearly identified and addressed, whilst also recognising the benefits that mobile phones provide, such as increased safety.

1.2. Woodrush High School has established the following Acceptable Use Policy for mobile phones that provides teachers, support staff, students, parents and carers guidelines and instructions for the appropriate use of mobile phones during school hours.

1.3. Students, their parents or carers must read and understand the Acceptable Use Policy as a condition upon which permission is given to bring mobile phones to school.

1.4. The Acceptable Use Policy for mobile phones also applies to students during school trips and visits and extra-curricular activities both on and off the school site.

2. Rationale

2.1. Learning and Teaching

The school recognises that the use of mobile technologies is an accepted part of everyday life but that such technologies need to be used appropriately. There will be occasions when mobile technologies can enhance and aid Learning and Teaching and explicit guidelines will be given by the classroom teacher on these occasions.

2.2. Personal safety and security

The School accepts that parents and carers give their children mobile phones to protect them from everyday risks involving personal security and safety. This is especially true when children are travelling alone on public transport or commuting long distances to school. It is acknowledged that providing a child with a mobile phone gives parents reassurance that they can contact them in an emergency whilst on their way to and from school.

3. Responsibility

3.1. It is the responsibility of students who bring mobile phones to school to abide by the guidelines outlined in this document.

3.2. The decision to provide a mobile phone to their children should be made by parents or carers. It is incumbent upon parents to understand the capabilities of the phone and the potential use/mis-use of those capabilities.

3.3. Parents and carers should be aware if their child takes a mobile phone to school. It is assumed household insurance will provide the required cover in the event of loss or damage. The school cannot accept responsibility for any loss, damage or costs incurred due to its use.

3.4. It is the responsibility of school staff to remove a mobile phone from a student in cases where the mobile phone is being used inappropriately, against the guidelines of the Acceptable Use policy.

3.5. Parents and carers are reminded that in cases of emergency, the school office is the point of contact and can ensure your child is reached quickly and assisted in any relevant way. Parents and carers should not contact their children via their mobile phone.

4. Acceptable Uses

4.1. Mobile phones should be switched off and kept out of sight during the school day unless clearly instructed to by the class teacher for use in Learning and Teaching (see below).

4.2. Mobile phones should be switched off and kept out of sight during break and lunchtime.

4.3. Mobile phones should not be used in any manner or place that is disruptive to the normal routine of the school.

4.4. On school trips and visits, students may use their mobile phones to contact parents with regards to accurate return times, for safe and prompt collection from school.

4.5. The school recognises the importance of emerging technologies present in modern mobile phones e.g. camera and video recording, internet access, MP3 and MP4 playback etc. Teachers or Support staff may wish to utilise these functions to aid Learning and Teaching and pupils may have the opportunity to use their mobile phones in the classroom. On these occasions, pupils may use their mobile phones in the classroom when express permission has been given by the Teacher or Support staff. The use of personal mobile phones in one lesson for a specific purpose does not mean blanket usage is then acceptable.

5. Unacceptable Uses

5.1. Unless express permission is granted, mobile phones should not be used to make calls, send messages, surf the internet, take photos or videos or use any other application during school lessons nor other educational activities, such as assemblies or trips and visits.

5.2. The Bluetooth function of a mobile phone must be switched off at all times and not be used to send images or files to other mobile phones.

5.3. Mobile phones must not disrupt classroom lessons with ring tones, music or beeping. They should be turned off during lesson times.

5.4. Using mobile phones to bully and threaten other students is unacceptable. Cyber bullying will not be tolerated. In some cases it can constitute criminal behaviour. If the use of technology humiliates, embarrasses or causes offence it is unacceptable regardless of whether ‘consent’ was given.

5.5. It is forbidden for students to use mobile phones to photograph or film any student or member of staff without their consent. It is a criminal offence to use a mobile phone to menace, harass or offend another person and almost all calls, text messages and emails can be traced.

6. Theft or damage

6.1. The school accepts no responsibility for lost, stolen or damaged mobile phones.

6.2. Students who bring a mobile phone to school should leave it in their bag when they arrive. To reduce the risk of theft during school hours, students who carry mobile phones are advised to keep them well concealed and not ‘advertise’ they have them.

6.3. Mobile phones that are found in the school and whose owner cannot be located should be handed to front office reception.

6.4. Students should mark their mobile phone clearly with their names.

6.5. The school accepts no responsibility for students who lose or have their mobile phones stolen while travelling to and from school.

6.6. It is strongly advised that students use passwords/pin numbers to ensure that unauthorised phone calls cannot be made on their phones (e.g. by other students, or if stolen). Students must keep their password/pin numbers confidential. Mobile phones and/or passwords may not be shared.

6.7. Lost and stolen mobile phones in the U.K. can be blocked across all networks making them virtually worthless because they cannot be used.

7. Inappropriate conduct

7.1. Mobile phones are banned from all examinations. Students must hand phones to invigilators before entering the exam hall. Any student found in possession of a mobile phone during an examination will have that paper disqualified. Such an incident may result in all other exam papers being disqualified.

7.2. Any student who uses vulgar, derogatory, or obscene language while using a mobile phone will face disciplinary action.

7.3. Students with mobile phones may not engage in personal attacks, harass another person, or post private information about another person using SMS messages, taking/sending photos or objectionable images, and phone calls. Students using mobile phones to bully other students will face disciplinary action. *[It should be noted that it is a criminal offence to use a mobile phone to menace, harass or offend another person. As such, the school may consider it appropriate to involve the police.]*

7.4. Students must ensure that files stored on their phones do not contain violent, degrading, racist or pornographic images. The transmission of such images is a criminal offence.

7.5 The production, distribution or forwarding on of any inappropriate images, videos or sound files that includes any student or member of staff, with or without their consent, is forbidden and could constitute a criminal offence.

8. Sanctions

8.1. Students who infringe the rules set out in this document could face having their phones confiscated by teachers. Students are required to hand over their phones immediately when requested to do so by any member of staff.

8.2. The use of a mobile phone in any area of school life, other than specified by a member of staff will result in the mobile phone will be removed from the student and placed in Student Services, where it can be collected by the student at the end of the day.

8.3. Should a mobile phone be used in lessons by a student for anything other than the explicit Learning and Teaching purpose as instructed by the class teacher, the mobile phone will be removed from the student and placed in Student Services, where it can be collected by the student at the end of the day.

8.4. If the same student has had their mobile phone removed from them more than 3 times in an academic year, the mobile phone will be held in Student Services until the students' parent or carer collects it in person and gives assurance that the student will no longer bring the phone into school.

Appendix 6 – Twitter Acceptable Use Policy

We have one main Twitter feed for the school that is just used to push information. This is open to anyone but the security settings are such that replies are not permitted.

Departments/clubs in school are allowed to set up Twitter accounts only under the following conditions

- E safety coordinator must be informed about the group and be a member so that monitoring can take place
- The group is private and so individuals must be approved by the staff member who set up the account.
- The Twitter account set up by the member of staff must not 'follow' any Twitter accounts of students or staff personal accounts.
- Only staff and current students can be part of the group.
- The following acceptable use statement must be displayed on the profile page 'Any use of this Twitter group is covered by the school ICT Acceptable Use Policy'
- Any unacceptable use must be reported immediately to the E safety coordinator