Woodrush High School

An Academy for Students Aged 11-18

ICT Policy

Policy author / reviewer	J Jarvis
Responsible LGB committee	Resources Committee
Date ratified	To be confirmed
Status	Statutory
Date of next review	every 3 years

The need for a policy

All Woodrush High School's information communication technology (ICT) facilities and information resources remain the property of Woodrush High School and not of particular individuals, teams or departments. By following this policy we will help ensure that ICT facilities are used:

- legally;
- securely;
- without undermining Woodrush High School;
- effectively;
- in a spirit of co-operation, trust and consideration for others;
- so that they remain available.

The policy relates to all ICT facilities and services provided by Woodrush High School, although special emphasis is placed on email and the internet. All employees (including volunteers and trainee teaches) and any other users of our IT are expected to adhere to the policy.

1. **Disciplinary measures**

1.1. Deliberate and serious breach of the policy statements in this section may lead to the Woodrush High School taking disciplinary measures in accordance with the Disaplinary Policy. Woodrush High School accepts that ICT – especially the internet and email system – is a valuable business tool. However, misuse of this facility can have a negative impact upon employees (including volunteers and trainee teachers) productivity and the reputation of the organisation.

1.2. In addition, all of the organisation's phone, internet and email related resources are provided for business purposes. Therefore, the organisation maintains the right to monitor the volume of internet and network traffic, together with the email systems. The specific content of any transactions will not be monitored unless there is a suspicion of improper use.

2. **Security**

2.1. As a user of Woodrush High School's equipment and services, you are responsible for your activity.

2.2. Do not disclose personal system passwords or other security details to other employees, (including volunteers and trainee teachers) or external agents, and do not use anyone else's log-in; this compromises the security of Woodrush High School. If someone else gets to know your password, ensure that you change it or get the Network manager to help you.

2.3. If you intend to leave your PC or workstation unattended for any reason, you should lock the screen to prevent unauthorised access. If you fail to do this, you will be responsible for any misuse of it while you are away. Logging off is especially important where members of the public have access to the screen in your absence.

2.4. Any pen drives or other storage devices used on Woodrush High School's network for the purpose of storing personal or sensitive data should be secure and only those that are the property of Woodrush High School should be used. Please see paragraph 7 for more detail.

2.5. Do not attempt to gain unauthorised access to information or facilities. The Computer Misuse Act 1990 makes it a criminal offence to obtain unauthorised access to any computer (including workstations and PCs) or to modify its contents. If you do not have access to information or resources you feel you need, contact the Head Teacher.

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

3. Use of Email

3.1. When to use email:

3.1.1. Use email in preference to paper to reach people quickly (saving time on photocopying / distribution) and to help reduce paper use.

3.1.2. Use the phone for urgent messages (email is a good backup in such instances). Use of email by employees (including volunteers and trainee teachers) of Woodrush High School is permitted and encouraged where such use supports the goals and objectives of Woodrush High School.

3.1.3. However, Woodrush High School has a policy for the use of email whereby employees and volunteers must ensure that they:

3.1.3.1. comply with current legislation;

3.1.3.2. use email in an acceptable way;

3.1.3.3. do not create unnecessary business risk to Woodrush High School by their misuse of the internet.

3.2. Unacceptable behaviour

3.2.1. Sending confidential information to external locations without appropriate safeguards in place. See paragraph 5 of this document for more details.

3.2.2. Distributing, disseminating or storing images, text or materials that might be considered indecent, pornographic, obscene or illegal.

3.2.3. Distributing, disseminating or storing images, text or materials that might be considered discriminatory, offensive or abusive, in that the context is a personal attack, sexist or racist, or might be considered as harassment or bullying.

3.2.4. Using copyrighted information in a way that violates the copyright.

3.2.5. Breaking into Woodrush High School's or another organisation's system, or unauthorised use of a password / mailbox.

3.2.6.Broadcasting unsolicited personal views on social, political, religious or other non-business related matters.

3.2.7.Transmitting unsolicited commercial or advertising material.

3.2.8.Undertaking deliberate activities that waste employee's effort or networked resources.

3.2.9. Deliberately or recklessly introducing any form of computer virus or malware into the corporate network.

3.3. Confidentiality

3.3.1.Always exercise caution when committing confidential information to email since the confidentiality of such material cannot be guaranteed. Woodrush High School reserves the right to monitor electronic communications in accordance with applicable laws and policies. The right to monitor communications includes messages sent or received by system users (employees, volunteers, trainee teachers and temporary employees) within and outside the system as well as deleted messages. See paragraph 5 for more detail.

3.4. General points on email use

3.4.1.When publishing or transmitting information externally be aware that you are representing Woodrush High School and could be seen as speaking on Woodrush High School 's behalf. Make it clear when opinions are personal. If in doubt, consult your line manager;

3.4.2.Check your inbox at regular intervals during the working day where practically reasonable. Keep your inbox fairly empty so that it just contains items requiring your action. Try to decide what to do with each email as you read it (e.g. delete it, reply to it, save the whole email in a folder, or extract just the useful information and save it somewhere logical);

3.4.3.Keep electronic files of electronic correspondence, only retaining what you need to. Do not print it off and keep paper files unless absolutely necessary;

3.4.4.Treat others with respect and in a way in which you would expect to be treated yourself (e.g. do not send unconstructive feedback, argue, or invite colleagues to make public their displeasure at the actions / decisions of a colleague);

3.4.5.Do not forward emails warning about viruses (they are invariably hoaxes and The IT technicians will probably already be aware of genuine viruses – if in doubt, contact them for advice);

3.4.6.Do not open an email unless you have a reasonably good expectation of what it contains, and do not download files unless they are from a trusted source. For example, do open **report.doc** from a colleague you know but do not open **explore.zip** sent from an address you have never heard of, however tempting. Alert IT Support if you are sent anything like this unexpectedly; this is one of the most effective means of Woodrush High School against email virus attacks.

3.5. Email signatures

3.5.1.Keep these short and include your name, title, phone / fax number(s) and website address.

4. Use of the Internet

4.1. Use of the Internet by employees (including volunteers and trainee teachers) is permitted and encouraged where such use supports the goals and objectives of the school.

4.2. However, when using the Internet, employees (including volunteers, and trainee teachers] must ensure that they:

4.2.1.comply with current legislation;

4.2.2.use the internet in an acceptable way;

4.2.3.do not create unnecessary business risk to the organisation by their misuse of the internet.

4.3. Unacceptable behaviour

4.3.1.In particular the following is deemed unacceptable use or behaviour by employees (including volunteers and trainee teachers) (this list is non-exhaustive):

4.3.1.1. Visiting internet sites that contain obscene, hateful, pornographic or other illegal material;

4.3.1.2. Using the computer to perpetrate any form of fraud, or software, film or music piracy;

4.3.1.3. Using the internet to send offensive or harassing material to other users;

4.3.1.4. Downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence;

4.3.1.5. Hacking into unauthorised areas;

4.3.1.6. Creating or transmitting defamatory material;

4.3.1.7. Undertaking deliberate activities that waste employees effort or networked resources;

4.3.1.8. Deliberately or recklessly introducing any form of computer virus into Woodrush High School’s network.

4.4. Chat rooms / instant messaging (IM)

4.4.1.The use of chat rooms and instant messaging is permitted for business use only. This use must have been agreed by the Head Teacher.

4.5. Obscenities / pornography

4.5.1.Do not write, publish, look for, bookmark, access or download material that might be regarded as obscene or pornographic.

4.6. Copyright

4.6.1. Take care to use software legally and in accordance with both the letter and spirit of relevant licensing and copyright agreements. Copying software for use outside these agreements is illegal and may result in criminal charges.

4.6.2. Be aware of copyright law when using content you have found on other organisations' websites. The law is the same as it is for printed materials.

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 E-safety co-ordinator in this school is 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/ PSHE lessons can be obtained from the E Safety Co-ordinator

5.2. Internet activity is monitored in school by use of the School internet filtering appliance system and data from this is reviewed on a daily basis. Virus protection is installed and updated regularly.

5.3. The school internet is provided by a safe and secure source – Currently BT broadband.

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. Confidentiality

6.1. If you are dealing with personal, sensitive and / or confidential information, then you must ensure that extra care is taken to protect the information and that it is only sent to the intended recipient.

6.2. If sending personal, sensitive and / or confidential information via email to a recipient not in the school ntweotrk, then the following protocols should be used. If there is any doubt as to the information being sent or the appropriate level of protection required, please check with the Network Manager.

6.2.1. Personal, sensitive and / or confidential information should be contained in an attachment;

6.2.2. In appropriate cases the attachment should be encrypted, and / or password protected;

6.2.3. Any password or key must be sent separately;

6.2.4. Before sending the email, verify the recipient by checking the address, and if appropriate, telephoning the recipient to check and inform them that the email will be sent;

6.2.5. Do not refer to the information in the subject of the email.

7. Woodrush High School’s network

7.1. Keep master copies of important data on Woodrush High School’s network server and not solely on your PC's local C: Drive or portable disks. Not storing data on Woodrush High School’s network server means it will not be backed up and is therefore at risk.

7.2. Ask for advice from the IT Technicians if you need to store, transmit or handle large quantities of data, particularly images or audio and video. These large files use up disk space very quickly and can bring the network to a standstill.

7.3. Be considerate about storing personal (non- Woodrush High School) files on Woodrush High School 's network.

7.4. Do not copy files that are accessible centrally into your personal directory unless you have good reason (i.e. you intend to amend them or you need to reference them and the central copies are to be changed or deleted) since this uses up disk space unnecessarily.

8. Removable media

8.1. If storing or transferring personal, sensitive, confidential or classified information using Removable Media you must;

8.1.1.Always consider if an alternative solution already exists;

8.1.2.Only use recommended removable media;

8.1.3.Encrypt and password protect;

8.1.4.Store all removable media securely;

8.1.5.Removable media must be disposed of securely by the IT Technicians.

9. Personal use of ICT facilities

9.1. Social media

For the purposes of this policy, social media websites are web-based and mobile technologies which allow parties to communicate instantly with each other or to share data in a public forum. They include websites such as Facebook, Twitter, Google+ and LinkedIn. They also cover blogs and image sharing websites such as YouTube and Flickr. This is not an exhaustive list and you should be aware that this is a constantly changing area.

9.1.1.Use of Social Media at work

9.1.1.1. Employees and volunteers are permitted to make reasonable and appropriate use of social media websites from Woodrush High School's IT equipment. You should ensure that usage is not excessive and does not interfere with work duties. Use should be restricted to your non-working hours, unless this forms part of your work responsibilities.

9.1.1.2. Access to particular social media websites may be withdrawn in the case of misuse.

9.1.1.3. Inappropriate comments on social media websites can cause damage to the reputation of the organisation if a person is recognised as being an employee (including volunteers and trainee teachers]. It is, therefore, imperative that you are respectful of the organisation's service as a whole including clients, colleagues, partners and competitors.

9.1.1.4. Employees [and volunteers] should not give the impression that they are representing, giving opinions or otherwise making statements on behalf of Woodrush High School unless appropriately authorised to do so. Personal opinions must be acknowledged as such, and should not be represented in any way that might make them appear to be those of the organisation. Where appropriate, an explicit disclaimer should be included, for example: '*These statements and opinions are my own and not those of* Woodrush High School.'

9.1.1.5. Any communications that employees (including Volunteers and trainee teachers) make in a personal capacity must not:

9.1.1.5.1. bring Woodrush High School into disrepute, for example by criticising clients, colleagues or partner organisations;

9.1.1.5.2. breach the Woodrush High School's policy on client confidentiality or any other relevant policy;

9.1.1.5.3. breach copyright, for example by using someone else's images or written content without permission;

9.1.1.5.4. do anything which might be viewed as discriminatory against, or harassment towards, any individual, for example, by making offensive or derogatory comments relating to: age, disability, gender reassignment, race, religion or belief, sex, or sexual orientation;

9.1.1.5.5. use social media to bully another individual;

9.1.1.5.6. post images that are discriminatory or offensive (or links to such content).

9.1.2. Woodrush High School maintains the right to monitor usage where there is suspicion of improper use.

9.2. Other personal use

9.2.1. Use of facilities for leisure or personal purposes (e.g. sending and receiving personal email, personal phone calls, playing computer games and browsing the internet) is permitted so long as such use does not:

9.2.1.1. incur specific expenditure for Woodrush High School;

9.2.1.2. impact on the performance of your job or role (this is a matter between each member of employees (including volunteers and trainee teachers) and their line manager);

9.2.1.3. break the law;

9.2.1.4. bring Woodrush High School into disrepute;

9.2.1.5. detrimentally affect the network performance by using large amounts of bandwidth (for instance by downloading / streaming of music or videos);

9.2.1.6. impact on the availability of resources needed (physical or network) for business use.

9.2.2. Any information contained within Woodrush High School in any form is for use by the employee (including volunteers and trainee teachers) for the duration of their period of work and should not be used in any way other than for proper business purposes, or transferred into any other format (e.g. loaded onto a memory stick / pen drive), unless necessary for business use, and with prior agreement of the Data Protection Officer.

10. Portable and Mobile ICT Equipment

10.1. This section covers items such as laptops, mobile devices and removable data storage devices. Please refer to paragraph 7 of this document when considering storing or transferring personal or sensitive data.

10.2. Use of any portable and mobile ICT equipment must be authorised by the Network Manager before use.

10.3. All activities carried out on Woodrush High School's systems and hardware will be monitored in accordance with the general policy.

10.4. Employees (including volunteers and trainee teachers] must ensure that all data belonging to Woodrush High School is stored on Woodrush High School's network and not kept solely on a laptop. Any equipment where personal data is likely to be stored must be encrypted.

10.5. Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of the car before starting your journey.

10.6. Synchronise all locally stored data, including diary entries, with the central organisation network server on a frequent basis.

10.7. Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades.

10.8. The installation of any applications or software packages must be authorised by the Network Manager, fully licensed and only carried out by him or an IT technician.

10.9. In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight.

9.10. Portable equipment must be transported in a protective case if one is supplied.

11. Remote Access

10.1. If remote access is required, you must contact the IT Technicians to set this up.

10.2. You are responsible for all activity via your remote access facility.

10.3. Laptops and mobile devices must have appropriate access protection, i.e. passwords and encryption, and must not be left unattended in public places.

10.4 To prevent unauthorised access to Woodrush High School's systems, keep all dial-up access information such as telephone numbers, logon IDs and PINs confidential and do not disclose them to anyone.

10.5. Select PINs that are not easily guessed, e.g. do not use your house or telephone number and do not choose consecutive or repeated numbers.

10.6. Avoid writing down or otherwise recording any network access information where possible. Any information that is written down must be kept in a secure place and disguised so that no other person is able to identify what it is.

10.7. Protect Woodrush High School's information and data at all times, including any printed material produced while using the remote access facility. [Take particular care when access is from a non-office environment].

10.8. Users of laptops and mobile devices are advised to check their car and home insurance policies for the level of cover in the event of equipment being stolen or damaged. Appropriate precautions should be taken to minimise risk of theft or damage.

10.9. Care should be taken when working on laptops in public places (e.g. trains) that any employee or client details are not visible to other people.

10 Electronic monitoring

10.1 You may find that you have access to electronic information about the activity of colleagues. Any such information must not be used by unauthorised individuals to monitor the activity of individual employees in any way (e.g. to monitor their working activity, working time, files accessed, internet sites accessed, reading of their email or private files, etc.) without their prior knowledge. Exceptions are:

10.1.1 In the case of a specific allegation of misconduct, when the Data Protection officer can authorise accessing of such information when investigating the allegation;

10.1.2 When the Network Manager cannot avoid accessing such information while fixing a problem, but this will only be carried out with the consent of the individual concerned.

11 Online purchasing

11.1 Any users who place and pay for orders online using personal details do so at their own risk and Woodrush High School accepts no liability if details are fraudulently obtained whilst the user is using Woodrush High School's equipment.

12 Care of equipment

12.1 Do not rearrange the way in which equipment is plugged in (computers, power supplies, phones, network cabling, modems etc.) without first contacting the Network Manager.

13 **Incident reporting**

13.1 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 Head of Year or member of the Senior Leadership Team that he considers that there has been a breach in the use of the School's computer system.

The Headteacher 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.

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

13.3 All E-safety incidents will be logged on SIMS

14 Agreement

All employees, volunteers, trainee teachers, contractors or temporary employees who have been granted the right to use Woodrush High School's ICT systems are required to sign this agreement confirming their understanding and acceptance of this policy.

Signed:		**Signed:**	
Manager:		**Employee [/volunteer]:**	
Date:		**Date:**	

Appendices

Appendix 1 – Student Acceptable Use Policy

- I will only use ICT systems in school, including the internet, e-mail, digital video and mobile technologies for school 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 following the school ICT security system and not reveal my passwords to anyone and change them 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 someone 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 into disrepute.
- 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 will respect the privacy and ownership of others' work on-line 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 (including 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 SNT school E-safety coordinator or RDC school network manager.

- I will only use the school's email / Internet / Intranet / Learning Platform 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 e-mail address, to students.
- I will only use the approved, secure e-mail system(s) 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 hardware of software without permission of RDC
- 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 code of conduct and to support the safe and secure use of ICT throughout the school

Signature ……………………………….. Date …………………..

Full Name ……………………………………………………………….......(printed)

Job title ………………………………………………………………….

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.

General Data Protection Regulation 2018

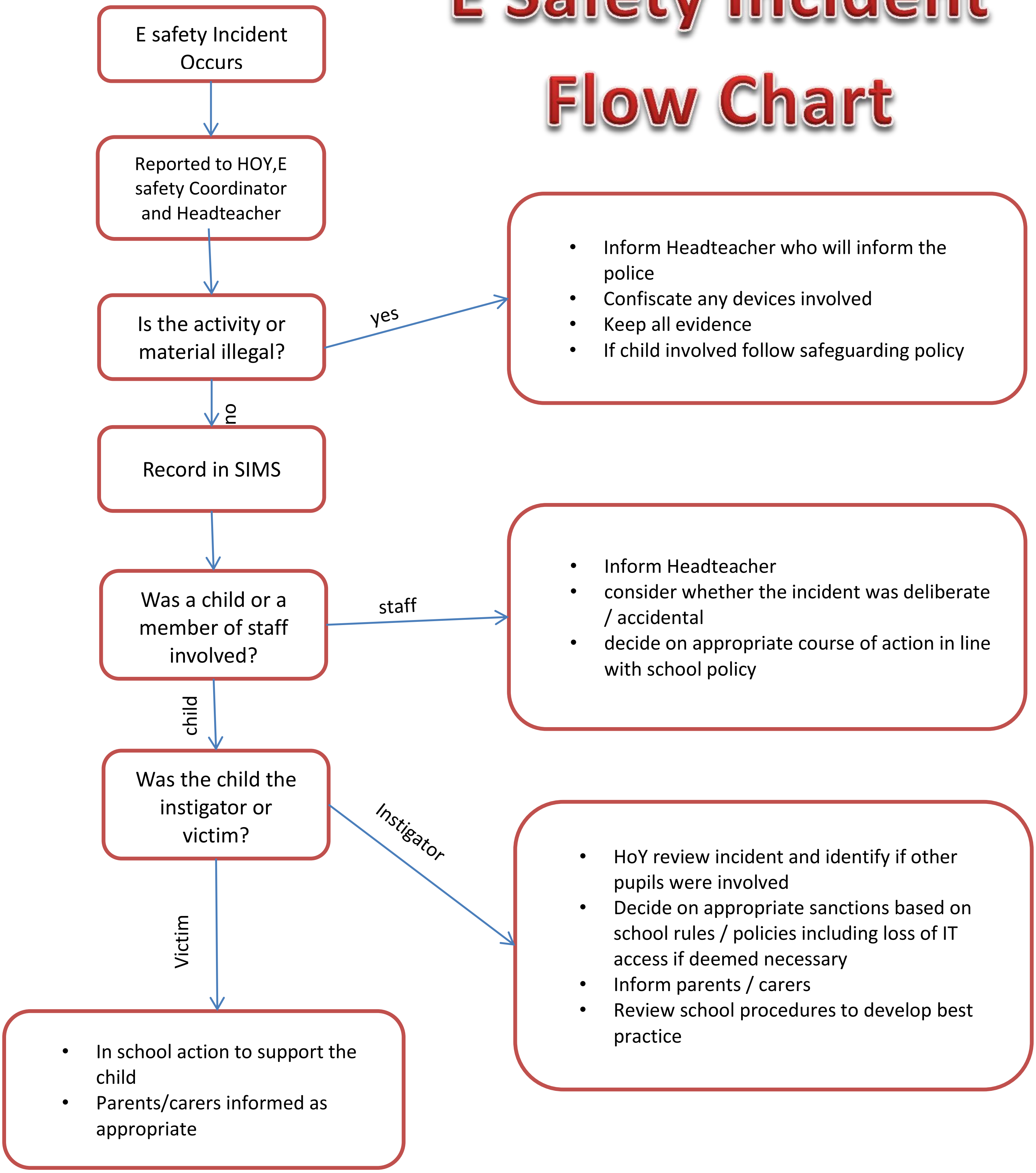
The Criminal Justice and Public Order Act (1994)
This Act extends the scope of the Obscene Publications Act 1959 to make the storage and electronic transmission of obscene material arrestable offences.

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.

Appendix 4 – E Safety Incident Flow Chart

E Safety Incident Flow Chart



E safety Incident Occurs

Reported to HOY,E safety Coordinator and Headteacher

Is the activity or material illegal?

yes

- Inform Headteacher who will inform the police
- Confiscate any devices involved
- Keep all evidence
- If child involved follow safeguarding policy

no

Record in SIMS

Was a child or a member of staff involved?

staff

- Inform Headteacher
- consider whether the incident was deliberate / accidental
- decide on appropriate course of action in line with school policy

child

Was the child the instigator or victim?

Instigator

- HoY review incident and identify if other pupils were involved
- Decide on appropriate sanctions based on school rules / policies including loss of IT access if deemed necessary
- Inform parents / carers
- Review school procedures to develop best practice

Victim

- In school action to support the child
- Parents/carers informed as appropriate

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, 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, 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 classroom lessons and while moving between lessons, 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, blogging etc. In the future teachers 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. 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 use any other application during school lessons and 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.

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

- SNT 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 teacher 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 SNT