WOODBRIDGE SCHOOL

Online Safety Policy – Whole School

Version Number:	V 6.2
Applies to:	Whole School (including EYFS)
Author (s):	Deputy Head (Pastoral), Online Safety Lead
Review Frequency:	Annual
Policy category (1, 2, 3, 4):	2
Last reviewed:	Trinity Term 2024
Next review due by:	Trinity Term 2025
Approved on (date):	Ed Comm: 12.06.24
Committee (s) Responsible:	Education
References (including legal and others eg ISBA).	DfE Preventing and Tackling Bullying: DfE: Supporting children and young people who are bullied: Advice for Schools; DfE Keeping Children Safe in Education; DfE Searching, Screening and Confiscation; https://www.gov.uk/government/collections/using-technology-in-education
ISI Reg:	7
Other related policies and documents:	KCSIE 2023; Data Protection Policy; Acceptable Use Policy (within this Online Safety Policy); EYFS Policy; Safeguarding & Child Protection Policy; Anti-Bullying Policy; Complaints Policy; Staff Code of Conduct; Health and Safety Policy; PSHE

Contents

1. Introduction & scope

1.1 This policy applies to all members of the school community (including staff, pupils, parents, visitors) who have access to and are users of school ICT systems, both in and out of the school.

1.2 The School will deal with online safety incidents in accordance with the procedures outlined in both this policy and in associated school policies, such as the safeguarding and child protection, behaviour and anti- bullying policies. It will, where known and appropriate, inform parents of incidents of inappropriate online safety behaviour that take place out of school.

2. Roles and Responsibilities

Governors

2.1 The Education Committee is responsible for the approval of this policy and for reviewing its effectiveness.

There is a nominated governor responsible for liaison with the DSL and Online Safety Lead.

Head

2.2 The Head has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety is delegated to the DSL and Online Safety Lead.

Designated Safeguarding Lead

2.3 The Designated Safeguarding Lead (DSL) is responsible for ensuring the School meets the digital and technology standards in schools and colleges - Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK (www.gov.uk). The DSL is trained in online safety issues and is aware of the potential for serious child protection / safeguarding issues to arise from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate on-line contact with adults/strangers inc Prevent
- Potential or actual incidents of grooming
- Cyber-bullying.

Online Safety Lead

2.4 The online safety Lead takes day-to-day responsibility for online safety issues and helps in establishing and reviewing the school online safety policies/documents. Other responsibilities include:

- Ensuring all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- Liaising with school technical staff
- The Online Safety lead is currently the DSL

The Head of IT Services is responsible for assisting the DSL in ensuring the School meets the digital and technology standards in schools and colleges - Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK (www.gov.uk) as well as ensuring the following:

2.5.1 That the school's technical infrastructure is secure and is not open to misuse or malicious attack.

2.5.2 That users may only access the school's networks and devices if properly authenticated and authorised.

2.5.3 The filtering policy is applied and updated on a regular basis.

2.5.4 That they keep up to date with online safety technical information in order to carry out their online safety role effectively and to inform and update others as relevant.

2.5.5 That the use of the school's networks and devices is monitored to ensure compliance with the Acceptable Use Policies (AUPs) in order that any misuse or attempted misuse can be identified and reported to the appropriate person for investigation.

2.5.6 That systems are kept up to date

Teaching and Support Staff are responsible for ensuring that:

2.6.1 They have an up to date awareness of online safety matters and of the current Online Safety policy and practices. This includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring.

2.6.2 They have read, understood and agreed to the Staff AUP agreement.

2.6.3 They report any suspected misuse or problem to the appropriate person for investigation.

2.6.4 All digital communications with other staff, pupils and parents are on a professional level.

2.6.5 They help pupils understand and follow the Online Safety and acceptable use policies.

2.6.6 They help pupils acquire a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

2.6.7 They monitor the use of devices in lessons and other school activities (where allowed) and implement current policies with regard to these devices.

Pupils – at an age appropriate level

2.7.1 Are responsible for using the school digital technology systems in accordance with the Pupil AUP Agreements

2.7.2 Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

2.7.3 Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.

2.7.4 Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions.

2.7.5 When pupils are participating in online lessons, the same high standard of behaviour is expected.

Parents

2.8 Parents play a crucial role in ensuring that their children understand the need to use the Internet / mobile devices in an appropriate way. Parents are asked to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events.
- Access to the Parent Portal.
- Their children's personal devices in the school (where allowed)

3. Policy Statements

Education – Pupils

3.1 Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, and will be provided in the following ways:

- An online safety curriculum is provided as part of, PSHE and other lessons and is regularly revisited
- Key online safety messages are reinforced as part of a planned programme of assemblies, talks, lessons, tutorial activities
- Pupils are taught to be critically aware of the materials and content they access on-line and be guided to validate the accuracy of information
- Pupils are helped to understand the need for the Pupil AUP agreement and encouraged to adopt safe and responsible use both within and outside school
- Pupils are helped to understand the benefits and risks associated with social media, online posting and messaging
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics that would normally result in internet searches being blocked. In such a situation, staff can request IT Services Support to remove those sites from the filtered list for those pupils. Any request to do so should be audited by the Head of IT Services, and clear reasons for the need must be established and recorded.

Education – Parents

3.2.1 Parents play an essential role in the education of their children and in the monitoring / regulation of the children's online behaviour.

3.2.2 The School provides information and awareness to parents through sharing of information, seminars and other methods as appropriate.

Education and Training – Staff

3.3 It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned online course for online safety training will be made available to staff. An audit of the online safety training records of all staff will be carried out regularly
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school's online safety Policy and Acceptable Use Agreements
- This Online Safety Policy and its updates will be presented to and discussed by staff
- The Online Safety Lead will provide advice/guidance/training to individuals as required.

Technical – Infrastructure, Equipment, Filtering and Monitoring

3.4 The School will be responsible for ensuring that the school infrastructure is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

School technical systems will be managed in ways that ensure that it meets recommended technical requirements:

- There will be regular reviews and audits of the safety and security of School technical systems
- Where possible, infrastructure will be secured and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by the IT department. Users are responsible for the security of their username and password.
- Internet access is filtered for all users.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- Anyone using School IT Systems must be informed their usage is monitored
- All School systems will be appropriately protected from accidental or malicious activity, where possible. The systems should be security tested at least every other year.

Bring Your Own Device (BYOD)

3.4.1 Users who connect their own devices to the school's network are bound by the school's policies and filtering and monitoring.

3.4.2 The school adheres to the principles and complies with the requirements of the Data Protection Act.

3.4.3 All users are provided with and accept the relevant AUP agreement.

3.4.4 All school network systems are secure.

3.4.5 Devices connected to the school's network are covered by the school's normal filtering systems.

3.4.6 IT Services will provide instructions on how to connect devices to the school Wi-Fi. These connections are recorded and monitored.

3.4.7 Pupils receive guidance on the appropriate use of personal devices.

Use of Digital and Video Images

3.5.1 When using digital images, staff should inform and educate pupils about the implications of the taking, use, sharing, publication and distribution of images. In particular, they should recognise the implications of publishing their own images on the internet e.g. on social networking sites.

3.5.2 Under the General Data Protection Regulations (GDPR) any digital image where a person or persons are clearly identifiable will be classed as 'personal data' and therefore restricted by the GDPR rules – please refer to the School's Data Protection Office (DPO).

3.5.3 Certain uses of images are necessary for the ordinary running of the School; other uses are in the legitimate interests of the School and its community and unlikely to cause any negative impact on children. The School is entitled lawfully to process such images and take decisions about how to use them, subject to any reasonable objections raised.

3.5.4 Consent is given via signing the parental contract to the School indicating agreement to the school using images of pupils as set out in this policy. The parent should contact the School if this becomes unacceptable. However, parents should be aware of the fact that certain uses of their child's images may be necessary or unavoidable (for example if they are included incidentally in CCTV or a photograph).

3.5.5 We hope parents will feel able to support the School in using pupil images to celebrate the achievements of pupils, sporting and academic; to promote the work of the School; and for important administrative purposes such as identification and security.

3.5.6 Any parent who wishes to limit the use of images of a pupil for whom they are responsible should contact the Head's PA in writing. The School will respect the wishes of parents/carers (and indeed pupils themselves) wherever reasonably possible, and in accordance with this policy.

3.5.7 Parents should be aware that, from around the age of 12 and upwards, the law recognises pupils' own rights to have a say in how their personal information is used – including images.

3.5.8 Parents, guardians or close family members (hereafter, parents) are welcome to take photographs of (and where appropriate, film) their own children taking part in School events, subject to the following guidelines, which the School expects all parents to follow:

- When an event is held indoors, such as a play or a concert, parents should be mindful of the need to use their cameras and filming devices with consideration and courtesy for cast members or performers on stage and the comfort of others. Flash photography can disturb others in the audience, or even cause distress for those with medical conditions; the School therefore asks that it is not used at indoor events.
- Parents are asked not to take photographs of other pupils, except incidentally as part of a group shot, without the prior agreement of that pupil's parents.
- Parents are reminded that such images are for personal use only. Images which may, expressly or not, identify other pupils should not be made accessible to others via the internet (for example on Facebook), or published in any other way.
- Parents are reminded that copyright issues may prevent the School from permitting the filming or recording of some plays and concerts. The School will always print a reminder in the programme of events where issues of copyright apply.
- Parents may not film or take photographs in changing rooms or backstage during School productions, nor in any other circumstances in which photography or filming may embarrass or upset pupils.

- The School reserves the right to refuse or withdraw permission to film or take photographs (at a specific event or more generally), from any parent who does not follow these guidelines, or is otherwise reasonably felt to be making inappropriate images.
- The School sometimes records plays and concerts professionally (or engages a professional photographer or film company to do so), in which case CD, DVD or digital copies may be made available to parents for purchase. Parents of pupils taking part in such plays and concerts will be consulted if it is intended to make such recordings available more widely.

Communications

3.6.1 A wide range of rapidly developing communications technologies has the potential to enhance learning.

3.6.2 When using communication technologies the School considers the following as good practice:

- Users should be aware that email communications are monitored and are not a secure method of communication..
- Staff and pupils should use School provided systems (email, Teams, itsLearning etc.) to communicate.
- Sensitive information should not be sent by email to anyone unless the message has been encrypted. Contact the IT Services Department for help with this.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents/guardians (email, social media, chat, blogs, itslearning, Teams etc) must be professional in tone and content. These communications may only take place on official (monitored) systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils are taught about online safety issues, such as the risks attached to the sharing of personal details. They are also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses and telephone numbers should be used to identify members of staff.

Social Media

3.7.1 The school encourages and supports staff in their use of digital technologies, sites and apps in the course of their work (teaching, extracurricular, pastoral) with pupils but requires that any such use is informed and fully consistent with our standards and policies.

3.7.2 There should be no communications between staff and pupils on personal social media. Electronic communications between staff and pupils should be conducted on school systems, such as school email, or the school virtual learning environment. Exceptions to this can only be made via application to the DSL.

3.7.3 When using personal social media accounts school staff should ensure that:

- No reference should be made in social media to pupils, parents/guardians or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

3.7.4 Official school social media accounts should have:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including
  - Systems for reporting and dealing with abuse and misuse
  - Understanding of how incidents may be dealt with under the schools disciplinary procedures

Unsuitable / inappropriate activities

3.8 Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from School and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The School believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in/or outside the school when using School equipment or systems. The School policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for Boarders in School House	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, datatransfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatredon the grounds of sexual orientation) - contrary to the Public Order Act 1986					X

	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filteringor other safeguards employed by the School					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use ofthe internet)					X	
On-line gaming (educational)		X	X			
On-line gaming (non-educational)			X		X	
On-line gambling					X	
On-line shopping / commerce		X	X		X	
File sharing		X	X			
Use of social media		S	X		X	
Use of messaging apps		S	X		X	
Use of video broadcasting e.g. Youtube		X	X			

S = Acceptable for staff

Responding to Incidents of Misuse

3.9 Reports of misuse of IT equipment and services may originate from these sources and by these means:

IT Services:

- Daily filter log reports.
- Routine examination of firewall and other service logs.
- Alerts raised from desktop monitoring software.

- Materials discovered during routine or other maintenance of School-owned IT equipment – including servers, desktop and laptop computers and mobile devices.
- As a result of observations of unusual patterns of network and storage use.

Through complaints concerning IT related activity made to the School from:

- Pupils
- Parents
- Staff
- Others outside the community

Line managers (in the case of staff) – or tutors (in the case of pupils):

- Suspicions of IT misuse by staff or pupils.
- Evidence handed to managers or tutors by other parties.

Individuals

- Staff members or pupils who wish to confess to some wrong-doing.

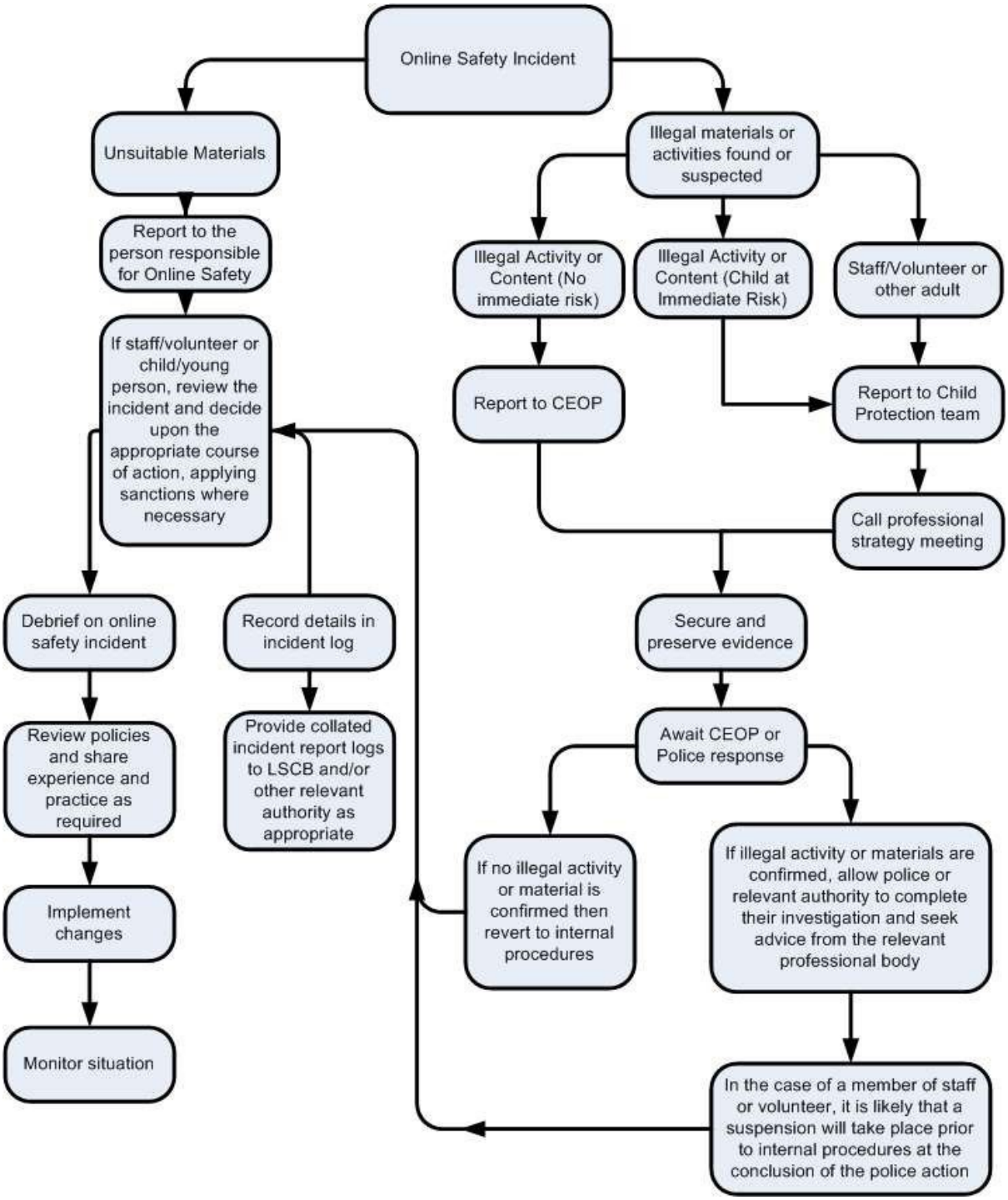
However, the incident is reported or discovered there are two broad courses of action that can be taken - depending entirely on whether there is any suspicion of illegality involved or not.

Illegal incidents

3.10 Anyone suspecting that:

- accesses have been attempted to any website containing child abuse images
- accesses have been attempted to any website containing material that breachesthe Obscene Publications Act
- accesses have been attempted to any website containing criminally racist material
- accesses have been attempted to any website which contains statements or images that are intended to radicalise people or in any other way endorse, condone or inciteextremist or terrorist activity
- any such materials are themselves to be found on any electronic device - whetherowned by the School or not
- there has been any incident by electronic means of 'grooming' behaviour

must report all allegations, complaints, concerns or suspicions directly to the DSL or Head (as appropriate), or, in their absence, to the Chairman of Governors, unless that person is the subject of the concern; those about the Head should be reported to the Chairman of Governors. All allegations, complaints, concerns or suspicions about the Chairman of Governors should be reported to the LADO without the Chairman of Governors being informed. The LADO may choose to appoint a 'case manager'.


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

Other Incidents

3.11 It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow School policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff/volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Police involvement and/or action

If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- promotion of terrorism or extremism
- other criminal conduct, activity or materials

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

4. Compliance and Monitoring arrangements

This policy will be subject to a thorough review process including consideration at the Education Committee on an annual basis. This will ensure that practice across the whole school is in line with this policy, the Complaints procedure and with current guidance and legislation.

Appendix A

ACCEPTABLE USE POLICY AGREEMENT FOR PUPILS

Scope of this Policy

This agreement is intended to encourage imaginative, responsible and safe use of digital technologies. By acting with care and thought pupils should be putting into practice much of this policy.

The school provides both networked, desktop computers and wireless access to the internet through the school's own filtered connection. Wireless access is available for use via your own devices.

It is standard practice in organisations to audit users' internet activity and all staff and pupils are audited in this way. Audit trails are examined when necessary. Should you find yourself looking at or opening material you consider the school would think inappropriate (or material you find disturbing), simply inform a member of staff so we can work with you to address the matter.

- I understand that the school will log and monitor my use of computers, devices and my digital communications

Identity and responsibility (online and digital)

This section applies to all your use of digital technologies, whether school-owned or personal.

In the digital realm, once something is posted online it has a persistence that is not like something that is said. It is also replicable and searchable (directly and through its metadata), and you cannot be sure who your audience is or will be. Once something is posted online, its effects are often magnified and can be mirrored out of context.

All of this requires experience to understand. Remember: when you post, you have not only your own reputation to consider but also that of others and that of the school. Every member of the community has to take responsibility for their actions online. If you are in doubt, it is best not to post, send an email, etc.

- I will respect and maintain the integrity of my own and others' digital identities
- I will log on only as myself
- I will keep my login details private and make them secure
- I will not leave any device logged in and accessible to others
- I will exercise informed judgement about disclosing my personal details and will not give out another person's details without their clear consent
- I will be polite and responsible when I communicate with others.
- I will not make, post or send images and video footage of others except with the agreement and understanding of those involved. Agreement must extend to the finished, edited product
- I understand that financial transactions are permitted provided that I act within the constraints of the school's rules and with my parents' approval.

- I understand that the school's computers and systems are not to be used to upload, download or access any materials which are illegal, or which endorse, condone, or incite illegal, extremist or terrorist activity or which are in any other way inappropriate for school, or likely to cause harm or distress to others, or bring the school's name into disrepute. I understand that I may not use any program or software to access such materials by bypassing the school's filters.

Network and hardware integrity

I will respect and maintain the network and the computers the school provides:

- I will not open unexpected or suspicious files.
- I understand the need to exercise judgement when connecting a device to the school's network or to a computer. Those with non-executable files on them are clearly fine, but those with executables (e.g. a browser designed to run safely from a USB stick) can be harder to assess. I will not store or seek to install any executable file on the school network.
- I will not link devices that are themselves computers (in whatever form) to the wired network without first consulting the Head of IT Services.
- I understand the need to exercise judgement when downloading files and am aware that viruses can be hidden in documents and images (for example) and not just in executable files. I will always seek advice if in doubt.
- I will respect the network's integrity when sending messages. I will not spam people or send needless messages. I will not attempt to send messages anonymously or pseudonymously for malicious purposes.
- I will report any actual or potential technical incident or security breach to the Head of IT Services.
- I understand that if I fail to observe this agreement I will be subject to disciplinary action.

I agree to comply with the rules and regulations set out in the School ICT Acceptable Use Policy Agreement for pupils.

Appendix B

ACCEPTABLE USE POLICY AGREEMENT FOR STAFF

This agreement is intended to encourage imaginative, responsible and safe use of digital technologies. By acting with care and thought you should be putting into practice much of this policy.

In the digital realm, once something is posted online it has a persistence that is not like something that is said. It is also replicable and searchable (directly and through its metadata), and you cannot be sure who your audience is or will be. Once something is posted online, its effects are often magnified and can be mirrored out of context. All of this requires experience to understand. Remember: when you post, you have not only your own reputation to consider but also that of others and that of the school. Every member of the community has to take responsibility for his or her actions online. If you are in doubt, it is best not to post, send an email, etc.

This Acceptable Use Policy is intended to ensure:

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

Access to ICT is made available to staff to enhance their work and to enhance opportunities for pupils' learning, and the school expects staff to be responsible users.

Acceptable Use Policy Agreement

- I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.
- I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT.
- In any interactions with pupils I will ensure appropriate use of ICT.
- I confirm that I have read and understood the School Online Safety Policy.

For my professional and personal safety:

- I understand the school may monitor my use of its ICT systems and networks.
- I understand that the rules set out in this agreement also apply to use of school ICT systems out of school, and to the transfer of personal data out of school.
- I understand that the security of my account is my responsibility and that I should
    - Logon only as myself;
    - Keep my login details private, keep make them secure and not share them with anyone;

        - Not leave any device logged in and accessible to others.

- I will report any actual or potential technical incident or security breach to the Head of IT Services.

- I will immediately report any illegal, inappropriate or harmful material I become aware of when in school or connected to the school network:

    - Material that appears to originate from sources external to the School should be reported to IT Services;
    - Material that appears to have been sent or circulated by a pupil or parent should be reported to the Designated Safeguarding Lead (DSL) (or in his absence a Deputy DSL)
    - Material that appears to have been sent or circulated by a member of staff (including a temporary member of staff or volunteer) should be reported to the Head.

I will be professional in my communications and actions when using school ICT systems at school, when using school ICT systems and equipment or when connected to the school network:

- I will ensure that when I take and / or publish images of others I will do so in accordance with the school's policy on the use of digital / video images.

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.

- Any use that I make of chat and social networking sites will be in accordance with the guidance given in the Staff Code of Conduct.

- I will not engage in any on-line activity that may compromise my professional responsibilities.

- I understand that the school ICT systems are primarily intended for educational use.

The school has the responsibility to provide safe and secure access to ICT:

- I will not open any hyperlinks in emails, or any attachments to emails, unless the source is known and trusted.

- I will not try to upload, download, or access any materials which are illegal (for example child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or which endorse, condone, or incite illegal, extremist or terrorist activity or which are in any other way inappropriate for school, or may cause harm or distress to others. I will not try to use any programs or software to bypass the school's filtering and security systems in order to access such materials.

- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the school's Data Protection Policy.

- I understand that data protection requires that any staff or pupil data to which I have access must be kept private and confidential.

- I will immediately report any damage, loss or faults involving school equipment or software to IT Support.

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 AUP Agreement applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises

- I am aware that emails may be disclosed as evidence in court and that, even if deleted, copies may exist on a back-up system
- I understand that if I fail to comply with this AUP Agreement, I could be subject to disciplinary action.

I agree to comply with the rules and regulations set out in School ICT Acceptable Use Policy Agreement for staff.

Appendix C

ACCEPTABLE USE POLICY AGREEMENT FOR VISITORS

I understand that I must use the school's systems and devices, including its wireless network, in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users.

- I understand that my use of the school's systems and devices and digital communications will be monitored.
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- Whilst in the school, I will not try to upload, download or access any materials which are illegal (for example child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or which endorse, condone, or incite illegal, extremist or terrorist activity or which are in any other way inappropriate for school, or may cause harm or distress to others. I will not try to use any programs or software to bypass the school's filtering and security systems in order to access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the Head of IT Services
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I will not access, copy, remove, add to or otherwise alter any other user's files, without permission.
- I will not install or attempt to install programs of any type on a school device, nor will I try to alter school computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened, to the Head of IT Services.

I understand that if I fail to comply with this agreement the school has the right to remove my access to school systems and devices.

I agree to comply with the rules and regulations set out in School ICT Acceptable Use Policy Agreement for visitors.

Signed: Name: Date:

Appendix D

Quick Reference Social Media Guidelines

These guidelines are for ALL members of staff about the use of pupil images and names on social media.

- Use pupil first names only (inc when with a picture).
- Consider how important an identifiable image is
- Make sure the image is less identifiable (e.g., group picture with no reference to who, for example John is, or a photo of them conducting the activity from a distance)
- With external media (newspapers etc) full names may be used but only after parents are consulted and have given consent.

EYFS

• No names of pupils for children at Woodbridge School Prep/Woodbridge School Pre-Prep in EYFS years (birth – 5 years old).

If you have any questions, please contact either:

- Designated Safeguarding Lead.
- Director of Operations (also School DPO).
- Woodbridge School Head.
- Woodbridge School Prep and Pre-Prep Head.
- Woodbridge School Prep Deputy Head.
- Online Safety Lead.
- Marketing.