WANSTEAD HIGH SCHOOL

E-Safety & Acceptable Use Policy

Person Responsible	Mr Z Ali
Review Frequency	Every 2 years
Last Reviewed	June 2021
Next Review Date	Autumn Term 2026/2027
Committee	Behaviour & Personal Development
Ratified by Full Governing Body on	30 September 2024
This policy is communicated by the following means	School Website

Contents

Policy statement

E-safety may be described as a school's ability to protect and educate the school community in their use of information and communications technology (**ICT**) and to have the mechanisms in place to intervene and support any incident where appropriate.

Safeguarding is a serious matter; at Wanstead High School we use ICT and the internet extensively across all areas of the curriculum. Online safeguarding, known as E-Safety, is an area that is constantly evolving, and as such this Policy will be reviewed every two years or an annual basis or in response to a serious e-safety incident, whichever is sooner.

The purpose of this E-Safety Policy (the **Policy**) is twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to a pupil member of staff, or liability to the school.

This Policy also incorporates the following more specific policies as appendices:

- Staff Social Media Policy (Appendix A)
- Staff Acceptable Use Policy (Appendix B)
- Pupil & Parent Social Media Policy (Appendix D)
- Pupil Acceptable Use Policy (Appendix E)

This Policy should be read together with the school's Behaviour Policy.

This Policy takes into account the following legislation and guidance:

- Data Protection Act 2018
- Computer Misuse Act 1990
- Human Rights Act 1998
- Education Act 2011
- Freedom of Information Act 2000
- The Education and Inspections Act 2006
- Keeping Children Safe in Education 2025
- Searching, screening and confiscation: advice for schools 2022

Policy governance (roles & responsibilities)

Governing Body

The Governing Body is accountable for ensuring that WHS has effective policies and procedures in place; as such it will review this Policy at least every two years and in response to a serious e-safety incident to ensure that:

- it is up to date;
- it covers all aspects of ICT use within the school;
- e-safety incidents are appropriately dealt with; and
- it is effective in managing e-safety incidents.

Governors are required to follow the staff Social Media Policy (Appendix D) and staff ICT Acceptable Use Policy (Appendix E), as well as having regard to the guidance for school governors on online social networking produced by the National Coordinators of Governor Services (NCOGS) (Appendix G).

Headteacher

The Headteacher has overall responsibility for e-safety within WHS. The day-to-day management of e-Safety is delegated to a member of staff, the Assistant Head leading on Digital Strategy (the **Assistant Head (E-safety)**) or the Designated Safeguarding Lead (**DSL**), as appropriate.

The Headteacher will ensure that:

- E-safety training and awareness is planned and up-to-date and appropriate to the recipient (e.g. pupils, staff, senior leadership team, Governing Body, parents).
- The Assistant Head (e-Safety) has had appropriate training to undertake the day-to-day duties.
- All E-safety incidents are dealt with promptly and appropriately.

Assistant Head (e-Safety)

The Assistant Head (e-Safety) with the support of the Network Manager will:

- Keep up to date with the latest risks to children whilst using ICT.
- Familiarise themselves with the latest research and available resources for school and home use.
- Review this Policy regularly and raise any matters requiring attention to the Headteacher.
- Advise the Headteacher and Governing Body on all e-safety matters.
- Engage with parents and the school community on e-safety matters at school and/or at home.
- Work with the Network Manager to ensure any technical e-safety measures in school (e.g. internet filtering software, behaviour management software) are fit for purpose.
- Make themselves aware of any reporting function with technical e-safety measures (e.g. internet filtering reporting function).
- Liaise with the Headteacher and Governing Body to provide appropriate reports and data on e-safety.
- Retain overall responsibility for e-safety incident reporting.

IT Technical Support Staff

Technical support staff (including the Network Manager and the ICT Manager) are responsible for ensuring that the IT technical infrastructure is secure; this will include at a minimum:

- Anti-virus is fit-for-purpose, up to date and applied to all capable devices. Software updates are regularly monitored, and devices updated as appropriate.
- Any e-safety technical solutions such as Internet filtering are operating correctly.
- Filtering levels are applied appropriately and according to the age of the user.
- Categories of use are discussed and agreed with the Assistant Head (e-Safety) and Headteacher.
- Passwords are applied correctly to all users and are in accordance with up-to-date guidance on length and strength.
- The IT System has a secure password and access policy.

All Staff

All staff must ensure that they:

- Read and understand this Policy, and seek further information and guidance from the Assistant Head (e-Safety) as required.
- Seek opportunities to support and promote e-safety across interactions with pupils.
- Ensure that the pupils are aware of, and adhere to, the guidelines contained within the Pupil & Parent Social Media Policy and the Pupil ICT Acceptable Use Policy when working online in their classes or in their care.
- Report any e-safety incident to the Assistant Head (e-Safety), or in their absence to the Headteacher. If unsure, raise the matter with the Assistant Head (e-Safety) or Headteacher to decide on next steps.
- Fully understand the reporting procedure for e-safety incidents.

Staff are only permitted to access the school network, systems or ICT equipment if they act in accordance with this Policy (including the staff Social Media Policy and the staff Acceptable Use Policy). All new staff must sign the Confirmation Statement at Appendix C to confirm they have read and understand this Policy.

Pupils

- E-safety is embedded into the curriculum - pupils will be given the appropriate advice and guidance by staff, in all subject areas across the curriculum.
- Pupils must ensure they are aware that they can report concerns about e-Safety to an adult in school.
- All pupils must comply with the Pupil & Parent Social Media Policy and the Pupil ICT Acceptable Use Policy at Appendices D and E to this Policy.
- Any failure to comply with those pupil policies will be dealt with in accordance with the school's Behaviour Policy.

Pupils are only permitted to access the school network, systems or ICT equipment if they act in accordance with this Policy (including the Pupil & Parent Social Media Policy and the Pupil Acceptable Use Policy). All new Year 7 pupils and their parents (and any pupils and their parents who join the school after this time) must sign the Confirmation Statement at [Appendix E] to confirm that they have read the Pupil & Parent Social Media Policy and the Pupil Acceptable Use Policy.

Parents / Carers

- Parents play the most important role in the development of their children; as such the school seeks to ensure that parents have access to resources to acquire the skills and knowledge they need to ensure the e-safety of children outside the school environment. The school will use parents' evenings, school newsletters and free online training courses

to keep parents up to date with new and emerging e-safety risks, and will involve parents in strategies to ensure that pupils are empowered to understand the risks they face.

- Parents must also understand that the school needs to have to rules in place to ensure that their child can be properly safeguarded. As such new pupils and their parents/carers must sign a Confirmation Statement to confirm that they have read the Pupil & Parent Social Media Policy and the Pupil Acceptable Use Policy before the pupils will be permitted access to the school network, systems or ICT equipment.

Network and device management

WHS uses a range of devices including desktop computers, laptops and tablets. To safeguard pupils and to prevent loss of data we employ assistive technology. The school makes use of the SENSO cloud-based platform for device monitoring and management, which can track and monitor staff and pupil use of school systems.

Internet filtering

We use a Smoothwall web filter that prevents unauthorised access to illegal websites, including those sites deemed inappropriate under the Prevent agenda (a UK-wide strategy that aims to stop people becoming terrorists or supporting terrorism). It also prevents access to inappropriate websites: what is appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The Assistant Head (e-Safety) and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher. Web access is logged indefinitely for all users of the ICT systems in our school.

Email filtering

We use Google Suite and Office 365 technology that mitigates the risk of infected email being sent from the school, or being received by the school. Infected is defined as an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message. The system is also used to filter certain words and can be used for monitoring.

Passwords

Staff and pupils are unable to access the network without a unique username and password. Staff and pupil passwords should be changed if there is a suspicion that it has been compromised. The Network Manager will be responsible for ensuring that passwords are changed on a regular basis or as and when required. The use of another person's credentials at any time is forbidden.

Anti-virus

All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. The Network Manager is responsible for ensuring this task is carried out, and will report to the Assistant Head (e-Safety) if there are any concerns.

Safe use

School network & the internet

Access to the school network and systems, including access to the internet, is a privilege, not a right.

New staff will be granted access once they have completed and returned the Confirmation Statement at Appendix C to this Policy.

New pupils will be granted access once they and their parents/carers have completed and returned the Confirmation Statement at Appendix F to this Policy.

All pupils and parents will be able to access this E-safety Policy through the school's website, and are expected to comply with those sections relevant to them.

This Policy apply to all staff and pupils, whether access to the school network or internet is through a school or personal device, by cable or wireless, on school premises or off the school site, in the UK or abroad, whether during or outside of school hours, and on any device, laptop or PC, either school-owned or personal.

Email

Staff are permitted to use the school email system, and as such will be given their own email address, based on their network username. The log-in credentials for that account must not be shared with others. Staff are reminded that:

- The school's email service to be used for professional work-related emails only.
- The use of personal email addresses for communicating with pupils is not permitted: when communicating with pupils, Staff should only use the systems provided and managed by the school, which includes the Managed Learning Environment and school email accounts.
- The school may be required to disclose staff emails in responses to requests made by parents and others under the Freedom of Information Act (known as subject-access requests or SARs).

Pupils are permitted to use the school email system, and as such will be given their own email address, based on their network username. The log-in credentials for that account must not be shared with others. Pupils are reminded that:

- They should use their school email account only for School-related activity as set out in the Pupil ICT Acceptable Use Policy (Appendix E).
- They must immediately tell a teacher if they receive an offensive or inappropriate email.
- They must not reveal personal details about themselves or others in email communication, or arrange to meet anyone without specific permission from an appropriate adult.
- It will not generally be appropriate or necessary to share their school email address outside of the school community except in specific circumstances, and they should consult a responsible adult if they are in doubt about doing so.

Photos and videos

All parents/cares are requested to sign a photo release slip on their child's entry to the school, as part of the Induction Pack they receive. Non-return of the photo release slip will not be assumed as acceptance of photo release.

Social networking

WHS is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community. However, any subject specific social media services, permitted for use within WHS must have been appropriately risk assessed, managed and moderated in accordance with the staff Social Media Policy and Pupil & Parent Social Media Policy before they can be permitted for use within WHS.

In addition, with reference to images that may be uploaded to such sites, the following is to be strictly adhered to by the school:

- Permission slips (either as hard copy filed in the pupil record folder or as flagged on the pupil record on SIMS) must be consulted before any image or video of any child is uploaded to ensure that photo release consent is held.
- There is to be no identification of pupils using full names: first name and year group only is to be used, if at all.
- All images, videos and other visual resources that are not originated by the school will not be used unless the owner's permission has been granted. Permission to use copyrighted resources must be sought and received before they are used.

Notice and take down policy

Should it come to the school's attention that there is a resource which has been inadvertently uploaded, either to the school website or a school/department authorised social networking site, and the school does not have copyright permission to use that resource, it will be removed as quickly as possible.

Reporting e-safety incidents

Where there is a concern that an e-safety incident has occurred which places a pupil/s at risk of harm this should be reported as a safeguarding concern by emailing childprotection@wansteadhigh.co.uk The DSL will liaise with The Assistant Head (e-Safety) and appropriate action will be taken to safeguard the pupil/s and to address any breaches of policy. All staff should make themselves aware of the procedures and the responsible staff involved in this process.

Please refer to Wanstead High School's Safeguarding & Child Protection Policy section on reporting incidents (page 6).

Training and curriculum

It is important that the wider school community is sufficiently empowered with the knowledge to mitigate risk while using digital technology; this includes updated awareness of new and emerging issues. WHS seeks to provide this awareness by regular distribution of e-safety information to staff, pupils and parents.

The Assistant Head (e-Safety) is responsible for recommending a programme of training and awareness for the school year to the Headteacher for consideration and planning. The Assistant Head (e-Safety) arranges an annual programme of online e-safety training for appropriate staff, to be incorporated within the CPD programme, and Governing Body. This online e-safety training provides staff with a certificate which must be renewed by further training on an annual basis. This continuous rolling training programme means that staff will always be up to date with the latest issues on e-safety from new and evolving technologies.

The Assistant Head (e-Safety) school shall ensure that aspects of e-safety for pupils is firmly embedded into the curriculum.

Whenever ICT is used in the school, staff must ensure that pupils are made aware about the safe use of technology and risks as part of the pupil's learning. If asked, Heads of Department should be able to demonstrate where and how the awareness of risk is imparted to pupils in lessons.

As well as the programme of training, the Assistant Head (e-Safety) will establish further training or lessons as necessary in response to any e-safety incidents.

Should any member of staff feel they have had inadequate or insufficient training generally or in any area this must be brought to the attention of the Assistant Head (e-Safety) or Headteacher for consideration of further training or CPD.

Unofficial channels as a forum for parents' views

It is entirely natural for parents/carers to discuss school life and express their thoughts and opinions with others face to face or on the phone. The school recognises that there will be occasions where, for whatever reason, parents/carers may not agree with a particular course of action or may have specific concerns.

However, some of these conversations take place through, for example, WhatsApp groups and are now also being aired on social media, and the person posting has little control over who might ultimately see it. Some of the comments and observations expressed could cause offence if aired in the public domain, and may in some cases be intimidating or even slanderous.

This is not to suggest that the school and its staff are above criticism or do not welcome feedback. However, it is always best when this is constructive and reasonable and is focused on finding an acceptable solution. When difficult things need to be said, it is usually best to do so face-to-face, or at least in some form of private communication with the school, such as an email or letter, to avoid the risk that discussion on sensitive topics gets out of hand.

Ill-considered use of social media can exacerbate incidents and issues, and cause school staff to spend a disproportionate amount of time trying to manage issues and situations. The school and its staff would much prefer it if this time could be focused on pupils' education.

The Pupil & Parent Social Media Policy at Appendix D sets out more guidance for parents.

Disciplinary and consequences

Any breaches of this Policy – including any of the appended Policies - by staff may result in disciplinary action and may, in serious circumstances, result in suspension or dismissal from the school.

Any breaches of this Policy by a pupil may result in consequences applied in accordance with the school's Behaviour Policy, of which this Policy forms an important part.

Any breaches of this Policy by a parent/carer may be contacted by the school to discuss the issue and seek to resolve any concerns. Repeated or severe violations may result in further actions, including restrictions on participation in school activities.

Monitoring and review

The Headteacher and the Assistant Head (e-Safety) overseeing the school's Digital Strategy monitor the implementation of this Policy (and its appendices), including ensuring that it is updated to reflect the needs and circumstances of the school.

The Policy is put before the Governing Body at least every two years and in response to a serious e-safety incident to ensure that:

- it is up to date;
- it covers all aspects of ICT use within the school;
- e-safety incidents are appropriately dealt with; and
- it is effective in managing e-safety incidents.

Appendix A: Staff Social Media Policy

1. Introduction and Scope

This Policy sets out the appropriate use of social media by the staff of WHS. Our aim is to create a safe and positive environment that promotes respectful and responsible use of social media within the framework of the school's E-Safety Policy through:

- assisting staff to understand what is acceptable and what is not when using social media inside and outside of school;
- explaining the responsibilities of staff in guiding pupils to work online safely and responsibly; and
- mitigating the risk of malicious allegations against staff and others who have online contact with pupils.

Except where more specific applications are given, this policy applies to all staff of WHS, which includes teachers, associate staff, governors and all who work on the school site, including volunteers, where their work brings them into contact with the pupils. New staff are required to sign and return to the school the Confirmation Statement at Appendix C to the school's E-Safety Policy before they will be permitted to access the school network, systems or ICT equipment.

This Policy is to be read together with the Pupil & Parent Social Media Policy and the Pupil ICT Acceptable Use Policy at Appendices D and E to the school's E-Safety Policy. Staff must ensure that the pupils in their care are aware of, and adhere to, the guidelines contained within those pupil policies when working online in their classes or in their care.

2. What is social media?

'Social media' includes any interactive online media that allows parties to communicate with one another or share information. Examples include Twitter, Facebook and LinkedIn, but also blogs, video and image-sharing websites such as YouTube, Snapchat, Instagram, Tumblr and Flickr.

Social media for the purposes of this Policy also **includes closed groups such as WhatsApp**. This is because, although these are private groups, participants are not able to control the flow of information from these groups, and comments made on them have the potential to be shared more widely in a manner akin to social media.

Be aware that there are many, many more examples of social media. This is a constantly developing and rapidly changing area of communication. You must act in accordance with this Policy in relation to any social media that you use, in relation to the undertaking of your professional duties and in relation to how the implications of your personal online activity may impact on your professional life.

3. Using social media and other online activity in school or with school ICT equipment

Certain use of social media in a professional capacity and in an educational context is acceptable. In fact, you are encouraged to explore innovative use of new technologies provided appropriate safeguards are taken.

However, when in school, you must not access social media sites or engage in other online activity in a personal capacity using the school's computers or other school devices at any time unless authorised to do so by a member of the senior leadership team.

While you may use your own (non-school issued) computer or other devices to access social media sites or engage in other online activity:

- outside of your classroom lesson times; AND
- when you are confident that a pupil will not be able to see or hear that activity.

Excessive use of social media, including interacting with social media on mobile phones while teaching or otherwise interacting with pupils, or which could be considered to interfere with professional duties, may be considered a disciplinary matter.

4. Using social media and other online activity outside of school

The school appreciates that staff will wish to make use of social media in a personal capacity, and does not seek to prevent or restrict appropriate personal use of social media. However, you must be aware that there are risks to the school and to you and others in the school community from inappropriate personal use of social media.

You may be recognisable or identifiable online, even where you use a pseudonym. As such, your online activity may be associated with the school when you are acting in your personal capacity. That means that if you express opinions or share information then those opinions or information may be attributed to the school.

If those opinions or information is not appropriate, then it may result in damage to the reputation of the school and others in the school community.

The easiest way to avoid this is:

- not to make any references mentioning the school by name or otherwise providing information which may identify the school or any of its staff, pupils or other members of the school community (e.g. job title); and
- not to make any statements which carry such risk - or if it is important to you to do so, then you should include a clear statement such as *"These are my own opinions and not those of my employer"*.

Be aware that all opinions or information you share or post, regardless of whether you have followed the above guidelines, must not do any of the following:

- bring the school into disrepute;
- breach confidentiality;
- breach copyright or other intellectual property restrictions;
- bully, harass or be discriminatory in any way; or
- be defamatory or derogatory.

Prior to joining the school, new staff should check any information they have placed on social media sites and remove any statements that might cause embarrassment or offence.

5. General social media guidance (both in and out of school)

Those working with children have a duty of care and therefore are expected to adopt high standards of behaviour to retain the confidence and respect of colleagues, pupils and parents/carers (and others in the school community) both within the school and outside of it.

You must maintain appropriate boundaries and manage personal information effectively so that it cannot be misused by third parties (e.g. for identify theft, of 'cyber bulling'). As such, when using social media, you should:

- never share log-in details or passwords;
- restrict access to certain groups of people (e.g. to your family and friends); and
- use the tightest privacy settings possible.

You must not make 'friends' or otherwise connect with pupils of the school over social media as this could potentially be construed as 'grooming', nor should you accept invitations to become a 'friend' or connection of any pupils.

You must keep any communications with pupils and parents/carers transparent and on a professional basis by only by using your school email address, not a personal account.

- If a pupil contacts you through social media or another non-official school channel, you must report this as a safeguarding concern by emailing childprotection@wansteadhigh.co.uk
- If a parent/carer contacts you using social media or a non-official school channel, you must direct them to contact you or the school through official school channels.

If you receive, or become aware that another member of staff has received, a communication from a pupil which may be inappropriate, you should immediately report this as a safeguarding concern by emailing childprotection@wansteadhigh.co.uk. If you are concerned that another member of staff has engaged with a pupil via social media you must report this concern to the Headteacher.

6. Guidance for encouraging e-Safety with pupils

Ensuring that pupils are safe when working online, either in school or at home, is a priority for all staff at WHS, including non-teaching staff. This is to be achieved not by 'locking down' access to the internet, but by ensuring we make pupils aware of the risks the internet may contain so that they can make informed judgements for their own safety, for themselves.

Ofsted categorises e-safety into 3 areas of risk:

- Content – being exposed to illegal, inappropriate or harmful material.
- Contact – being subjected to harmful online interaction with other users.
- Conduct – personal online behaviour that increases the likelihood of harm.

Ensure that you are aware of what is required of our pupils under the Pupil & Parent Social Media Policy and the Pupil ICT Acceptable Use Policy at Appendices D and E to the school's E-Safety Policy. You must ensure that the pupils in your care are aware of, and adhere to, the guidelines contained within those pupil policies when working online in your classes or in your care.

To keep themselves safe online, both in school and at home, you should encourage pupils to:

- use websites recommended by the teacher initially and be wary of unfamiliar links;
- consider who created a website and possible bias within information;
- email only people they know and exercise caution before opening an email sent by someone they don't know;
- use Internet chat rooms, websites, instant messaging, etc. with caution and know how to block and report unwanted users;
- use a pseudonym or nickname which doesn't allow them to be identified when using games or websites on the internet;
- never give out any personal information about themselves, friends or family online (including but not limited to home address, email or mobile number);
- never post or share their school name or a picture of them in school uniform (even to a friend);
- never arrange to meet anyone alone, always meet in a public place, and always tell an adult first;
- only use a webcam or phone camera with people they know (not including people they have met online);
- tell an adult they trust immediately if they encounter anything they are unhappy about or concerned with;
- report concerns via childprotection@wansteadhigh.co.uk ;
- avoid using websites that they would not feel comfortable talking to an adult about; and
- be aware comments they make on social media can be viewed by others – including private or closed group such as WhatsApp where they have no control over what others share.

7. Creating school social media channels

The school already has several social media accounts, and you are encouraged to make use of these, sharing announcements, achievements, resources or other content that may be useful or interesting to the school community with our Social Media Manager.

If you are interested in creating a new social media site for educational use in-school, you must first discuss this with the Assistant Head (e-Safety) before taking any action. You must also discuss the proposed post/content with, and get authorisation from, your Head of Department. The method and timing of the content monitoring process needs to be agreed, as well as the proposed content and proposed membership. All this information (and other relevant notes from discussions) should be written up, shared, agreed on and filed for future reference (either electronically or hard copy).

The following guidelines - together with any additional requirements provided by the Assistant Head (e-Safety) - will apply to any such accounts and the use of those accounts:

- Be aware of the setup settings before you allow the channel or site to go 'live', particularly the privacy settings.
- You must ensure that the site is private and cannot be accessed by anyone else, other than the intended members, without invitation.
- You must ensure that no content is posted on or shared to or through the channel or site which does, or has the potential to:
  - bring the school into disrepute;
  - breach confidentiality;

- breach copyright or other intellectual property restrictions;
- bully, harass or be discriminatory in any way; or
- be defamatory or derogatory.

- You will be responsible for monitoring and maintenance to the channel or site, including:
  - moderating all content posted on or shared to or through (whoever posts or shares it) the channel or site;
  - removing any inappropriate content; and
  - suitably restricting the membership.

If you have any questions or need technical assistance on setting up appropriate controls, you must seek the help of the ICT Manager.

Appendix B: Staff ICT Acceptable Use Policy

1. Introduction and Scope

This Policy outlines the acceptable use of the school's ICT and applies to all staff of WHS.

ICT is an integral part of the way our school works, and is a critical resource for pupils, staff, governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the school. However, the ICT resources and facilities our school uses also pose data protection, e-safety and safeguarding risk. This policy aims to:

- assist you to understand what is acceptable and what is not when using school ICT;
- support the school's related policies in relation to data protection, e- safety, social media and safeguarding;
- prevent disruption to the school through the misuse, or attempted misuse, of ICT systems; and
- explain your responsibilities in guiding pupils in safe and effective ICT use.

New staff are required to sign and return to the school the Confirmation Statement at Appendix C to the school's E-Safety Policy before you will be permitted to access the school network, systems or ICT equipment.

This Policy is to be read together with the staff Social Media Policy at Appendix A to the E-Safety Policy, as well as the Pupil ICT Acceptable Use Policy at Appendix E to the school's E-Safety Policy, and you must ensure that the pupils are aware of, and adhere to, the guidelines contained within the Pupil ICT Acceptable Use Policy when using ICT in your classes or while in your care.

2. Definitions

ICT facilities: includes all the school's facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service.

Materials: files and data created using the school's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs.

3. Examples of unacceptable use

Unacceptable use of the school's ICT is not permitted. The following actions are examples of unacceptable use of the school's ICT facilities:

- Breaching the school's policies and procedures.
- Breaching copyright or other intellectual property rights. *(See section on Copyright below.)*
- Bullying or harassment.
- Promotion of unlawful discrimination.
- Any illegal conduct, or statements which are deemed to be advocating illegal activity.

- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate.
- Activity which defames or disparages the school, or risks bringing the school into disrepute.
- Sharing confidential information about the school, its pupils, or other members of the school community.
- Connecting any device to the school's network without approval from the ICT Manager.
- Setting up any software, applications or web services on the school's network without approval from the ICT Manager, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data.
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from the ICT Manager.
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities.
- Causing intentional damage to the school's ICT facilities.
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission from the ICT Manager.
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation.
- Using inappropriate or offensive language.
- Promoting a private business or business interest.
- Using websites or mechanisms to bypass the school's filtering mechanisms.

This is not an exhaustive list. If you engage in any of the unacceptable activity listed above you may face disciplinary action, but the Headteacher will use professional judgement to determine whether there has been any other unacceptable usage of school ICT facilities when considering taking such action.

4. Exceptions from unacceptable use

Where the use of school ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the Policy may be granted at the Headteacher's discretion.

5. Access to school ICT facilities and materials

The school's ICT Manager manages staff access to the school's ICT facilities and materials. That includes, but is not limited to:

- Computers, tablets and other devices.
- Access permissions for certain programmes or files.
- The school provides unique Office 365 and Google logins that you must use when accessing the school's ICT facilities; in respect of which:
    - you must set strong passwords for their accounts and keep these passwords secure;
    - you must never share log-in details or passwords (you may face disciplinary action if you disclose account or password information); and
    - you are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

User access rights

All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices. These access rights are managed by the Network Manager:

- If you have access to files you are not authorised to view or edit, or need their access permissions updated or changed, contact the Network Manager (Dan Emerton).
- If you require access to files that you do not have access to, please contact the Network Manager.

You should not access, or attempt to access, systems, files or devices to which you have not been granted access. If access is provided in error, or if something is shared with you that you should not have access to, contact the Network Manager.

Internet access and content

You must not give the school Wi-Fi password to anyone who is not authorised to have it. Pupils are not permitted to use the school Wi-Fi unless specifically authorised and so you must not share the password with them. Doing so could result in disciplinary action.

The school wireless internet connection is secured. The school has a filtering system. You must report inappropriate sites that the filter has not identified and blocked (or appropriate sites that have been filtered in error) to the Network Manager.

You must always log out of systems and lock your ICT equipment when they are not in use to avoid any unauthorised access. School ICT equipment and systems should always be logged out of and closed down completely at the end of each working day.

6. Personal use of school ICT

Personal use of ICT facilities must not be overused or abused, and doing so may result in disciplinary action. You are permitted to occasionally use school ICT facilities for personal use
provided that such use:

- Does not take place during teaching hours.
- Does not constitute '**unacceptable use**' (as described above).
- Does not take place when pupils are present.
- Does not interfere with your job, or prevent other staff or pupils from using the facilities for work or educational purposes.

The ICT Manager may withdraw permission for personal use, or restrict access, at their discretion and at any time.

Be aware that:

- your personal use of the school's ICT facilities may bring your personal communications within the scope of the school's ICT monitoring activities. Where breaches of this Policy are found, disciplinary action may be taken.
- your personal use (even when not using school ICT facilities) can impact your employment by, for instance, putting personal details in the public domain, where pupils and parents/carers could see them.

You must follow the staff Social Media Policy at Appendix A to the E-Safety Policy when using social media to protect yourself online and avoid compromising your professional integrity.

7. Off-site access to the school's ICT

We allow staff to access to the school's ICT facilities and materials from outside school. The majority of WHS's systems are now cloud-based, for example Google Workspace, 4Matrix and Edulink.

When you are accessing the school's ICT facilities and materials virtually you must comply with the school's policies just as when you are accessing those the facilities and materials on the school site. You must be particularly vigilant when working off-site the school and take such precautions as the Network Manager may require from time to time against importing viruses or compromising system security.

Be aware that our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with the school's Data Protection and Breach Policy.

For that reason, we discourage you from accessing the school's ICT facilities in a public place unless absolutely necessary. If you do have to do so, you must:

- Never leave your computer or device unattended.
- Be aware of who is around you and make sure no-one (including any CCTV) can see your screen. Consider using a privacy filter which effectively blocks the view of your screen from people sitting either side of you.
- Not send or receive private information when using public Wi-Fi.
- Ensure that your computer or device is running any updates made available to it by the school before you use public Wi-Fi.

8. Accessing the school's ICT using your personal device

The school ensures that its own devices and systems have an appropriate level of encryption.

You may only use personal devices to access school data, work remotely, or take personal data (such as pupil information) out of school if you have been specifically authorised to do so by the Headteacher.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the Network Manager.

9. Use of email, phone and virtual meetings

Email:

- Use your school email account for work purposes only.
- Conduct all work-related business using your school email address - do not send any work-related materials to your personal email account, or use your personal email account to send work-related emails.
- Do not share your personal email addresses with parents/carers or pupils.
- Take care with the content of all email messages, as incorrect or improper statements can give rise to liability for matters such as discrimination, harassment and defamation.

- Email messages may be required to be disclosed in legal proceedings or in response to subject access requests (SARs) in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered; all email messages should be treated as potentially retrievable.
- Take extra care when sending sensitive or confidential information by email. Encrypt any attachments containing sensitive or confidential information so that the information is only accessible by the intended recipient.
- If you receive an email that was not meant for you, inform the sender and delete the email. If the email contains sensitive or confidential information, you must not make use of that information or disclose that information.
- If you receive an email which appears to be a phishing attempt, contact the Network Manager (do not forward the email unless the Network Manager tells you to, and do not click on any links).
- If you send an email in error which contains the personal information of another person, inform the Network Manager immediately and follow the data breach procedure in the school's Data Protection and Breach Policy.

Phone:

- Use phones provided by the school to conduct all work-related business.
- Do not use school phones for personal calls.
- Do not share your personal phone number with parents/carers or pupils.
- In exceptional circumstances, you may use your personal phone to contact pupils, but this must be done only as a last resort or in cases where safeguarding is a factor, such as on school trips. Withhold your phone number when contacting a pupil or parent/carer it if is possible to do so.

Virtual meetings and sessions:

- Staff must abide by the online protocols included in the Wanstead High School Guidance and Expectations for Remote Learning on the school website.
- Staff will aim to ensure that all tasks and activities that the pupils undertake during periods of remote learning are safe. Pupils are expected to carefully follow the instructions of their teacher during lessons.
- All staff follow the whole school Behaviour Policy with regard to discipline and classroom management face to face and whilst on line.
- Pupils are expected to join the remote session on time and to behave with respect and courtesy throughout the lesson.
- Pupils must only join Google Meets using their school.
- Just like a normal lesson pupils have been reminded to remain sensible, and respect members of staff. Behave appropriately in the same manner as you would during a face to face lesson.
- Pupils must mute (turn off) their microphones unless asked to unmute by the teacher chat (if enabled).
- All comments made by pupils must be focused on the work and be relevant to the lesson being taught.
- In every remote learning scenario, the expectation is for pupils to complete their work set to a high standard and to submit work to meet the deadline set.
- When working remotely, within Google Meets pupils can use direct message options to comment on their work, to ask questions or to seek further teacher guidance.

- Tutors can see the comments so pupils must write in an appropriate way at all times i.e. use academic English at all times.
- At no point, should pupils take any form of recording or photo or screen-shot of the session. If it is found that this has happened, it will immediately be referred to the behaviour team and pupils will face sanctions in line with our behaviour policy.
- When in a live session - pupils and any household member in view must be in appropriate clothes and have a neutral and appropriate background (e.g. appropriate setting and no siblings or other family members in the background).
- The rules regarding student use of technology are also outlined in the school's IT Acceptable User Agreement and are designed to help keep pupils and staff safe.
- Report any inappropriate or offensive pupils' behaviour in line with the school's behaviour and safety policy.

10. Monitoring of school network and ICT facilities

The school reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- internet sites visited;
- bandwidth usage;
- email accounts;
- telephone calls;
- user activity/access logs; and
- any other electronic communications.

The school monitors ICT use to:

- obtain information related to school business;
- investigate compliance with school policies, procedures and standards;
- ensure effective school and ICT operations;
- conduct training or quality control exercises;
- prevent or detect crime or behaviour that puts pupils or staff at risk; and
- comply with a subject access request (SAR) or any other legal obligation.

11. Security, software updates, firewalls, and anti-virus software

The school takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee security. You should always use safe computing practices when using the school's ICT facilities.

All the school's ICT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically. Make sure that you log out of school ICT equipment and systems at the end of each working day so updates can be installed.

You must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards the school implements to protect the school's ICT facilities and data.

You must ensure that any personal devices that you have been authorised to use for work purposes have effective and updated anti-virus software running before you access the school's network using it.

12. Data protection

All personal data must be collected, processed and stored in line with the school's Data Protection & Breach Policy.

13. Copyright

Many of the resources you find online are copyright protected, including music and video. You may only use all or part of a copyrighted work if you have the copyright owner's permission or if your use of the work falls under a legal exemption. Check the materials you are viewing for appropriate statements indicating copyright ownership and usage. It is your responsibility to respect these rights including all copyrights. Any copyright protected files found during routine checks will be removed and a warning will be given; repeat offenders may face disciplinary action.

Appendix C: Staff Confirmation - E-Safety Policy

To be completed and returned to the Network Manager. You will not be permitted to access the school network, systems or ICT equipment until you have done so.

- I have read and understand the school's E-Safety Policy, and the staff Social Media Policy and staff ICT Acceptable Use Policy appended to the E-Safety Policy.

- I have read and understand the Pupil & Parent Social Media Policy (Appendix D) and the Pupil ICT Acceptable Use Policy (Appendix E) and understand that I am responsible for:
  - seeking opportunities to support and promote e-safety across my interactions with pupils; and
  - ensuring that the pupils are aware of, and adhere to, the guidelines contained within the Pupil & Parent Social Media Policy and the Pupil ICT Acceptable Use Policy when working online in my classes or in my care.

- I have reviewed the content I have posted or shared on social media sites and removed any statements that are not in accordance with the staff Social Media Policy, and added a clear statement to existing posts as appropriate to the effect "*These are my own opinions and not those of my employer"*.

- I understand the need to promptly report any concerns about matters covered by the above policies.

- I understand that if I breach any of the above-named policies, then my access to the school network and systems will be immediately withheld pending investigation, and I may be required to immediately return any school ICT equipment.

- I understand that failure to act in accordance with the above-named policies may result in disciplinary action and may, in serious circumstances, result in my suspension or dismissal from the school.

Full Name of Staff (print):	Staff signature:
Department & Role:	Date:

Appendix D: Pupil & Parent Social Media Policy

1. Introduction and Scope

This policy outlines the appropriate use of social media for pupils and parents/carers of Wanstead High School. Our aim is to create a safe and positive environment that promotes respectful and responsible use of social media within the framework of the school's E-Safety Policy.

This policy applies to all pupils of WHS and their parents/carers. New Year 7 pupils and their parents are required to sign and return to the school the Confirmation Statement at Appendix F to the school's E-Safety Policy before they will be permitted to access the school network, systems or ICT equipment.

This policy should be read together with the Pupil ICT Acceptable Use Policy at Appendix E to the school's E-Safety Policy.

WHS staff are also responsible for ensuring that the pupils in their care are aware of, and adhere to, the guidelines contained within this policy.

2. What is social media?

'Social media' includes any interactive online media that allows parties to communicate with one another or share information. Examples include Twitter, Facebook and LinkedIn, but also blogs, video and image-sharing websites such as YouTube, Snapchat, Instagram, Tumblr and Flickr.

Social media for the purposes of this policy also **includes closed groups such as WhatsApp**. This is because, although these are private groups, participants are not able to control the flow of information from these groups, and comments made on them have the potential to be shared more widely in a manner akin to social media.

Parents should be aware that there are many, many more examples of social media. This is a constantly developing and rapidly changing area of communication. Pupils of all ages should be made aware of and follow the guidelines in this Policy relation to any social media that they use, both in school and at home.

3. Guidelines for Pupils

Using social media in school

- **Don't use social media in school.** Do not access social media on school devices, or on your own devices while you are in school (noting that you must follow the school's policy if you bring a mobile phone into school).
- **Have academic integrity.** Do not use social media to cheat or plagiarise. Academic dishonesty can have serious consequences.

Respect and Responsibility

- **Respect others.** Always be respectful to teachers, classmates, and others online, and when referring to others online. Any form of cyberbullying, harassment, malicious or inappropriate comments (including in private messages or closed groups) will not be tolerated and may lead to consequences for you.
- **Represent yourself positively.** All activity on the web leaves an identifiable online footprint, an evidence trail. Be aware when using social media what impression you are giving others about you, and that this may be visible in the future when you are applying for a job or further education.
- **Represent the school positively.** Remember that your online actions reflect on the school. Think before you post or share, and consider the potential impact of your words and actions on others. Don't post or share anything that could damage the school's reputation or the reputation of anyone in the School community.

Privacy and Security

- **Don't use social media if you are not old enough** (the permitted age is 13 for most sites including Facebook and Instagram).
- **Use privacy settings.** Set your social media accounts to private to control who can see your information and posts. Restrict access to only those people you know and trust.
- **Keep your account secure**. Don't share log-in details or passwords with anyone except your parents/carers (even your friends or siblings). Use strong, unique passwords for each of your social media accounts.
- **Protect personal information.** Never share personal information such as your address, phone number, school name or any other private details online, even if you think you know the person you are sharing it with.
- **Don't accept invitations to be a 'friend' or connection** of anyone online unless you are completely sure you know who they are - people online may not be who they say they are, be the age they say they are or even the gender they say they are. Do not invite your teachers or other school staff to be your 'friend' on social media.

Appropriate Content

- **Don't post or share inappropriate content**. Do not post or share any content that is offensive, inappropriate, or illegal. This includes, but is not limited to, hate speech, violence, nudity, and any form of discrimination.
- **Respect privacy.** Don't take or share photos or videos of others without their explicit permission. Be mindful of how your posts might affect others.
- **Be careful using school information.** Don't post any confidential information related to the school, staff, or other pupils. Do not use the school logo or uniform inappropriately on social media.
- **Report concerns.** If you have any concerns about anything you see online, tell your parent/carer or email, childprotection@wansteadhigh.co.uk. The DSL will liaise with The Assistant Head (e-Safety) and appropriate action will be taken

4. Guidelines for Parents

Supervision and Monitoring

- **Actively monitor activity.** Be aware of what social media accounts your child has and the minimum permitted age for having these. Regularly monitor your child's social media activity (including on their mobile phone) to ensure they are following this Policy. Be aware of the platforms they use and who they interact with.
- **Educate on risks.** Educate your child about the potential risks and consequences of social media use, including cyberbullying, online predators, and the permanence of digital footprints.[1]

Communication

- **Appropriate channels.** Use official school communication channels for any school-related concerns or queries. Avoid addressing sensitive school matters on social media.
- **Respectful Interaction.** Do not engage in discussions about individual pupils or staff members on social media. Handle conflicts and concerns directly with the school through appropriate channels.

Appropriate Content

- **Don't post or share inappropriate content**. Do not post or share any content that is offensive, inappropriate, or illegal. This includes, but is not limited to, hate speech, violence, nudity, and any form of discrimination.
- **Don't post or share malicious content.** Do not post or share content about the school or any member of the school community which is malicious or could be perceived as malicious.
- **Respect privacy.** Don't take or share photos or videos of others without their explicit permission. Be mindful of how your posts might affect others.
- **Be careful using school information.** Don't post any confidential information related to the school, staff, or other pupils. Do not use the school logo or uniform inappropriately on social media.

Modelling Behaviour

- **Set a good example.** Model responsible and respectful social media behaviour for your child. Show them how to interact positively and responsibly online.
- **Impact awareness.** Be mindful of how your social media activity can impact the school community. Avoid posting anything that could harm the reputation of the school or member of the school community or cause conflicts.
- **Social media use at school.** Do not use social media on your own devices while on school premises, helping at school events or on school trips.

[1] For helpful information, see this practical guide for parents and carers whose children are using social media platforms was developed by Internet Matters, NSPCC, Parent Zone, and UK Safer Internet Centre: UKCIS Social media guide for parents and carers - Internet Matters

5. Reporting Issues

If you become aware of any inappropriate behaviour or content related to the school on social media, please report it to the school immediately. Provide as much detail as possible to help the school address the issue effectively.

6. Consequences

If a pupil does not follow this Policy, it may result in consequences for that pupil such as:

- not being allowed to access the school network/internet;
- detention;
- parent involvement;
- suspension or exclusion from school;
- involvement of external authorities;
- or other actions in accordance with the school's Behaviour Policy.

Such consequences shall be applied in accordance with the school's Behaviour Policy, of which this policy forms an important part.

Parents who do not adhere to this Policy may be contacted by the school to discuss the issue and seek to resolve any concerns. Repeated or severe violations may result in further actions, including restrictions on participation in school activities.

Appendix E: Pupil ICT Acceptable Use Policy

1. Introduction and Scope

This policy outlines the acceptable use of Information and Communication Technology (ICT) facilities at WHS to ensure a safe, respectful and productive learning environment. This policy applies to all pupils of WHS using school-owned or personal ICT devices (including computers, tablets, smartphones, and other electronic devices) while on school premises or engaged in school-related activities.

This Policy aims to:

- assist you to understand what is acceptable and what is not when using school ICT;
- support the school's related policies in relation to data protection, e- safety, social media and safeguarding;
- prevent disruption to the school through the misuse, or attempted misuse, of ICT systems;
- promote good digital citizenship in our pupils and develop each pupil's ability to keep themselves safe when using technology; and
- explain the responsibilities of parents/carers in guiding pupils in safe and effective ICT use.

This policy should be read together with the Pupil & Parent Social Media Policy at Appendix D to the school's E-Safety Policy.

New Year 7 pupils and their parents are required to sign and return to the school the Confirmation Statement at Appendix F to the school's E-Safety Policy before they will be permitted to access the school network, systems or ICT equipment.

2. Acceptable use of school ICT

You must:

- **Educational Use.** Use the school's ICT facilities for educational and school-related purposes only. You are not permitted to use online chat or play online games unless specifically authorised by a member of staff.

- **Account Security.** Access only your own accounts and respect the privacy of and security of others' accounts.

- **Digital Conduct.** Communicate respectfully and responsibly in all online interactions.

- **Reporting Issues.** Report any security concerns, inappropriate content, or suspicious activities to a teacher or other member of staff immediately.

- **Internet Safety.** Refrain from sharing personal information online or in emails, or savin personal information onto school drives.

- **Respect Facilities.** Treat the school's ICT facilities with respect: it is provided as a tool to help you with your education.

What are the school's ICT facilities? These include (but not limited to) network infrastructure, desktop computers, laptops, tablets, phones, music players, hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the school's ICT service.

3. Unacceptable use of school ICT

You must not:

- **Credential Compromise.** Share your username or password, or allow anyone else to use your accounts.

- **Inappropriate Content.** Access, download, or distribute any material that is inappropriate, offensive or illegal, including pornography, hate speech, or violent content.

- **Cyberbullying.** Use the school's ICT resources to bully, harass, or harm others. Any form of cyberbullying, harassment, malicious or inappropriate comments (including in private emails) will not be tolerated and may lead to consequences for you.

- **Security Breach.** Attempt to bypass, disable, or interfere with school security systems, content filters, or network operations. This includes introducing viruses or similar to the school's network which could harm the school's ICT facilities.

- **Unauthorised Access.** Access or attempt to access restricted areas of the school's network, other users' accounts, or confidential information without permission.

- **Commercial Use.** Use the school's ICT facilities for commercial purposes, personal financial gain, or non-educational activities such as gaming, social media unrelated to schoolwork, or streaming non-educational content.

- **Software Installation.** Install or use unlicensed software, apps, or utilities on school devices without explicit permission from ICT staff.

- **Plagiarise.** Use the school's ICT resources to cheat or plagiarise. Academic dishonesty can have serious consequences.

- **Damage or Tamper with Facilities.** You must not deliberately damage or vandalise any ICT equipment. You must not unplug any cables from the back of machines.

- **Waste Resources.** You must not intentionally waste resources, including printer ink and paper.

4. Digital Citizenship

Our expectations of you:

- **Good Behaviour.** You are responsible for good behaviour on the Internet, just as you are in a classroom or a school corridor.

- **Intellectual Property.** Respect intellectual property rights by not plagiarising or infringing on copyrights. Properly cite sources and obtain permissions where necessary.

  What is copyright? When a person or company creates material – be it a work of literature, art, music, film or broadcast – copyright gives that person the right to control the use of their material. Copyright is designed to protect the creator of the content, and is designed to inform who can copy, adapt or distribute that work without permission and when this is allowed. Copyright can protect several types of content including novels, computer programs, song lyrics, newspaper articles, music, photographs, maps, logos and film. Copyright also applies to any medium including the internet and applies to downloading, sharing, and streaming.

- **Digital Footprint.** Be aware of your digital footprint and the long-term impact of your online activities.

- **Privacy Protection.** Protect your own and others' personal information. Avoid sharing passwords, addresses, phone numbers, or other sensitive data.

- **Be Respectful.** Communicate respectfully and responsibly online. Be polite and appreciate that other people might have different views to your own. The use of strong language, swearing or aggressive behaviour is not allowed.

- **Seek Advice.** If there is anything in this policy that you do not understand, please speak to your Head of Year.

5. Monitoring and privacy

The school may monitor, inspect, copy, review or record any and all activity using the school's ICT facilities at any time and without prior notice.

Pupils should not expect privacy when using school ICT facilities. School personnel may inspect any files or data stored on school-owned devices or networks at any time.

6. Consequences

Access to the internet and other school ICT facilities is a privilege, not a right, and that access requires responsibility.

If you do not follow this Policy, it may result in consequences for you such as:

- not being allowed to access the school network/internet;
- detention;
- parent involvement;
- suspension or exclusion from school;
- referral to external authorities;
- or other actions in accordance with the School's Behaviour Policy.

Such consequences shall be applied in accordance with the school's Behaviour Policy, of which this Policy forms an important part.

Parents who do not adhere to this Policy may be contacted by the school to discuss the issue and seek to resolve any concerns. Repeated or severe violations may result in further actions, including restrictions on participation in school activities.

7. Guidance for parents/carers

- **Actively monitor activity.** Be aware of what your child is doing using school ICT Facilities when they are at home.

- **Educate on risks.** Educate your child about the potential risks and consequences of using ICT and online activity, including cyberbullying, online predators, and the permanence of digital footprints.[2]

- **Set a good example:** Model responsible and respectful use of ICT facilities for your child. Show them how to interact positively and responsibly online.

- **Appropriate channels.** Use official school communication channels for any school-related concerns or queries.

- **Reporting ICT issues.** If you become aware of any inappropriate behaviour or content using the school's ICT facilities, please report it to the school immediately. Provide as much detail as possible to help the school address the issue effectively.

[2] For helpful information, see this practical guide for parents and carers whose children are using social media platforms was developed by Internet Matters, NSPCC, Parent Zone, and UK Safer Internet Centre: UKCIS Social media guide for parents and carers - Internet Matters

Appendix F: Pupil & Parent Confirmation - E-Safety Policy

To be completed and returned to the school marked for the attention of the Network Manager. A pupil will not be permitted to access the school network, systems or ICT equipment until you have done so.

Parent/Carer:

- I have read and understand the E-Safety Policy, and the Pupil & Parent Social Media Policy and Pupil ICT Acceptable Use Policy appended to the E-Safety Policy). I agree to follow the guidelines and principles outlined in those Policies.

- I understand that my child will be required to use a range of technology, including the internet, to further their learning.

- I understand that the school will take all reasonable steps to ensure the safety of my child while they are using that technology, but that the school cannot be held responsible for the content of materials accessed through the internet.

- I understand that the school is not responsible for content in non-official school channels (including e.g. parent/carer WhatsApp groups) and that I should not post or share content in such channels which is not in accordance with the Pupil & Parent Social Media Policy.

- I understand the need to use official school communication channels to report my concerns.

Full Name of Parent/Carer (print):	Parent/Carer signature:
Date:	

Pupil:

- I understand that I am responsible for my actions, both in and out of school, and both in person and online.

- I understand that if I do not follow the Pupil & Parent Social Media Policy and the Pupil ICT Acceptable Use Policy, I may face consequences, which may include: not being allowed to access the school network/internet; detention; parent involvement; suspension or exclusion from school; involvement of external authorities; or other actions in accordance with the school's Behaviour Policy.

Full Name of Pupil (print):	Pupil signature:
Year & Tutor Group:	Date: