Whitley Bay High School

ESafety Policy

This policy applies to all members of the school community (including staff, students, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

This policy has been written in conjunction with the following key documents:

- Behaviour in schools - GOV.UK (www.gov.uk)
- Child Exploitation and Online Safety Website: http://ceop.police.uk
- DfE Keeping Children Safe in Education 2022 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1101454/Keeping_children_safe_in_education_2022.pdf
- DfE Keeping Children Safe Online Government Publication: Coronavirus (COVID-19): support for parents and carers to keep children safe online - GOV.UK (www.gov.uk)
- DfE Online safety in schools and colleges: questions from the governing board https://www.gov.uk/government/publications/online-safety-in-schools-and-colleges-questions-from-the-governing-board
- DfE Relationships Education, Relationships and Sex Education (RSE) and Health Education 2019 Guidance: https://www.gov.uk/government/publications/relationships-education-relationships-and-sex-education-rse-and-health-education
- ESafety documentation released by the Government and Local Authority in July 2020 regarding student laptops funded by the DfE for disadvantaged Year 10 students.
- Generative artificial intelligence (AI) in education - GOV.UK (www.gov.uk)
- Generative AI in Education Call for Evidence: Summary of Responses November 2023: https://assets.publishing.service.gov.uk/media/65609be50c7ec8000d95bddd/Generative_AI_call_for_evidence_summary_of_responses.pdf
- JCQ-AI-Use-in-Assessments-Protecting-the-Integrity-of-Qualifications.pdf. T
- Searching, Screening and Confiscation (publishing.service.gov.uk)
- SWGfl: https://swgfl.org.uk/resources/online-safety-policy-templates/
- Teaching Online Safety in School June 2019: https://www.gov.uk/government/publications/teaching-online-safety-in-schools
- The Education People: https://www.theeducationpeople.org/media/4472/online-safety-within-kcsie-2021.pdf
- Think u Know website (and App – from NCEA and CEOP) Thinkuknow - home
- UK Safer Online Centre Website: http://www.saferinternet.org.uk/
- 360 Degrees Safe website: https://360safe.org.uk/about-the-tool

- The document also makes reference to the following school policies available on our website here:
  - Anti-Bullying Policy
  - Behaviour Policy
  - Child Protection Policy
  - Exclusion Policy
  - Staff Code of Conduct Policy

Date created: [January 2024]

Next review date: [January 2025]

Contents Page

1.Scope of the ESafety Policy

This ESafety Policy outlines the commitment of Whitley Bay High School to safeguard members of our school community online in accordance with statutory guidance and best practice.

This ESafety Policy applies to all members of the school community (including staff, students, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site.

Whitley Bay High School will deal with such incidents within this policy utilising associated Behaviour and Anti-Bullying Policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

2. Policy development, monitoring and review

This e-safety policy has been developed by the Finance and Premises Governing Body working group made up of:

Headteacher

E-Safety Leader (Deputy Headteacher)

Staff including GDPR Lead

Governors of the Finance and Premises committee

3. Schedule for development, monitoring and review

3.i. This Online Safety Policy was approved by the Finance and Premises *governing body on:*	*23.1.24*
3.ii. The implementation of this Online Safety Policy will be monitored by:	E-Safety Deputy Headteacher / Network Manager / Curriculum and Student Affairs Committee and Senior Leadership Team.
3.iii.Monitoring will take place at regular intervals:	*Any major ESafety updates will be shared during half termly safeguarding lead (DSL) meetings.* *Other updates will be shared with the Governing Body during Full Governors.* *Policy to be reviewed annually.*

3.iv. The *governing body* will receive a report on the implementation of the ESafety Policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	As part of Safeguarding updates in Full Governors when necessary
3.v The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*January 2025*
3vi. Should serious online safety incidents take place, the following external persons/agencies should be informed:	Senior Leadership Team (SLT) – DSL (Designated Safeguarding Lead) / DpDSL (Deputy Designated Safeguarding Lead) Police Front Door LADO

4. Process for monitoring the impact of the ESafety Policy

4.i. The school will monitor the impact of the policy using:

- Logs of reported incidents on CPOMS
- Monitoring logs of internet activity (sites visited via Smoothwall)
- Internal monitoring data for network activity (Using Securus)
- Surveys / questionnaires of
- Students
- Parents / carers
- Low level staffing concerns recorded in Staff Safe
- Staff.

5. Policy and leadership

5.i Responsibilities

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals[1] and groups within the school.

5.iiHeadteacher and senior leaders

a. The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety. They are closely supported by the ESafety Lead at Whitley Bay High School.
b. The headteacher, DSL, DpDSLs are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff[1].
c. The headteacher is responsible for ensuring that the Online Safety Lead, technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
d. The ESafety Lead and Network Manager will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
e. The Senior Leadership Team will receive regular monitoring reports from the ESafety Lead.

5.iii. Governors

a. The DfE guidance "Keeping Children Safe in Education" states:

> "Governing bodies and proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children's welfare …. this includes … online safety"

b. Governors are responsible for the approval of the ESafety Policy and for reviewing the effectiveness of the policy. Guidance is available to Governors through the UKCIS document "Online Safety in Schools and Colleges – questions from the Governing Body".

[1] 1 See flow chart on dealing with online safety incidents in 'Responding to incidents of misuse' and relevant local authority/MAT/ HR/other relevant body disciplinary procedures.

c. The Finance and Premises and Curriculum and Student Affairs Committee will receive regular information about online safety incidents and monitoring reports as part of Safeguarding updates. The Governor in charge of Child Protection and ESafety will have a key role in monitoring and reviewing the effectiveness of the ESafety Policy. The role includes:

1. regular meetings with the Safeguarding lead (DSL)
2. regularly receiving (collated and anonymised) reports of online safety incidents
3. checking that provision outlined in the ESafety Policy (e.g. online safety education provision and staff training is taking place as intended)
4. reporting to relevant governors group/meeting
5. occasional review of the filtering change control logs and the monitoring of filtering logs (where possible).

The governing body will also support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

5.iv. ESafety Lead

The ESafety Lead will:

a. lead Online developments and updates in the half termly Safeguarding Team meeting
b. work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL), where these roles are not combined
c. take day-to-day responsibility for online safety issues, being aware of the potential for serious child protection concerns
d. have a leading role in establishing and reviewing the school Esafety policy
e. Work with the Personal Development lead to promote an awareness of and commitment to online safety education across the curriculum and beyond
f. liaise with Personal Development Lead to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
g. ensure that all staff are aware of the procedures that need to be followed in the event of an Esafety incident taking place and the need to immediately report those incidents in the same way as any safeguarding issue
h. receive reports of online safety incidents[2] including those from Securus alongside student, parents and community referrals. These will be logged using CPOMS to inform future online safety developments
i. provide (or identify sources of) training and advice for staff and governors via CPD, parents and carers via the Safeguarding and ESafety section of the website and students through the Personal Development Curriculum
j. liaise with the school IT Team, pastoral staff and support staff (as relevant)
k. meet regularly with the Safeguarding and ESafety governor to discuss current issues, review (anonymised) incidents and if possible, filtering and monitoring logs
l. attend relevant governing body meetings
m. report regularly to headteacher/senior leadership team

n. liaises with the local authority when relevant.

The school will log any serious situation in the same way as any bullying or child protection incident via CPOMS. Securus and Smoothwall record all incidents which can be accessed to report on student esafety behaviour.

5.v. Designated Safeguarding Lead (DSL)

5.v.a.The DfE guidance "Keeping Children Safe in Education" states:

> "The designated safeguarding lead should take lead responsibility for safeguarding and child protection (**including online safety**). This should be explicit in the role holder's job description." … Training should provide designated safeguarding leads with a good understanding of their own role, … so they … are able to understand the unique risks associated with **online safety** and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college."

5.v.b. The Designated Safeguarding Lead and the ESafety Lead roles are not combined at Whitley Bay High School but both post holders work closely in collaboration due to the safeguarding issues often related to online safety.

5.v.c. The Designated Safeguarding Lead should be trained in online safety issues and be aware of the potential for serious safeguarding issues to arise from:

1. sharing of personal data [2]
2. access to illegal/inappropriate materials
3. inappropriate online contact with adults/strangers
4. potential or actual incidents of grooming
5. online bullying.
6. Prevent Strategy and radicalisation
7. Sexting
8. Accessing and hacking into secure networks
9. County lines and use of the local Metro system
10. Cyber crime
11. abusive, harassing, and misogynistic messages
12. the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography, to those who do not want to receive such content.

Any of the above issues may fall into either the Behaviour or Safeguarding and Child Protection Policy and will be actioned in line with the recommendations of these documents.

[2] See 'Data Protection Policy' on the school website.

5.v.i. Curriculum Leads

Curriculum Leads will work with the ESafety Lead to, where relevant, supplement the work of the Personal Development Curriculum in delivering an online safety education programme. This will be provided through reference to their subject curriculum area where relevant, and:

a. An age appropriate mapped out Personal Development Curriculum
b. LEV lessons
c. Assemblies
d. The contextual 'Thought for the Week' and other pastoral programmes
e. Through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

5.vii.Teaching and support staff

School staff are responsible for ensuring that:

a. they have an awareness of current Esafety matters/trends and of the current school ESafety Policy and practices
b. they understand that Esafety is a core part of safeguarding
c. they have read, understood, and signed the Staff Acceptable Use Agreement (AUA) when they log onto their computer
d. they immediately report any suspected misuse or problem to The Safeguarding Team consisting of DSL and DpDSLs for investigation/action, in line with the school safeguarding procedures
e. all digital communications with students and parents/carers should be on a professional level and only carried out using official school systems using Office 365 Apps, but mainly Outlook and the @whitleybayhighschool.org email account. Personal email accounts and personal social media should not be used for school purposes
f. online safety issues are embedded in all aspects of the curriculum and other activities
g. ensure students understand and follow the ESafety Policy and Acceptable Use Agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
h. they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies ("away unless we say") regarding these devices. More information is available in Section 20 of this policy
i. in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
j. where lessons take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies and should take note of the guidance contained in the SWGfL Safe Remote Learning Resource. More information is available in section 23 of this policy

k. have a vigilant and prompt approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc in line with any child protection concern
l. they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of personal device and social media. Staff will receive training on this as part of annual Child Protection Training which is conducted on the second training day at the start of the academic year.

5.viii. Network manager and technical staff in the IT Team

The network manager and IT Team is responsible for ensuring that:

a. they are aware of and follow the school ESafety Policy to carry out their work effectively.
b. the school technical infrastructure is secure and is not open to misuse or malicious attack
c. the school meets (as a minimum) the required online safety technical requirements as identified by the local authority and DfE
d. there is clear, safe, and managed control of user access to networks and devices
e. they keep up to date with Esafety technical information in order to effectively carry out their ESafety role and to inform and update others as relevant
f. the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the Safeguarding Team for investigation and action
g. the filtering policy (via Securus) is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person
h. monitoring software/systems are implemented and regularly updated as agreed in school policies
i. monitoring and filtering occurs and takes place for DfE laptops that are loaned out to students who are working from home and accessing their own network via Intune. This includes ensuring the system that manages student laptops has up to date critical security patches installed to protect the devices from any issues. Critical patches must be applied a minimum of every half term.

5. vix IT Provider

At Whitley Bay High School, we work in conjunction with the local authority “North Tyneside Council” who provide our broadband and firewall, the school’s in house Network Manager and monitor firewalls and filtering using a Smoothwall Appliance.

The DfE Filtering and Monitoring Standards says:

“Senior leaders should work closely with governors or proprietors, the designated safeguarding lead (DSL), and IT service providers in all aspects of filtering and monitoring. Your IT service provider may be a staff technician or an external service provider.”

“Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL should work closely together with IT service providers to meet the needs of your setting. You may need to ask filtering or monitoring providers for system specific training and support.”

Our School IT Team provide the DSL daily Filtering and Monitoring Reports. Our schools in house IT Team is responsible for:-

a. maintaining filtering and monitoring systems
b. providing filtering and monitoring reports
c. completing actions following concerns or checks to systems”
d. Schools in house IT Team is responsible for:-

Schools IT Team work with the Senior Leadership Team and DSL to:

a. procure systems
b. identify risk
c. carry out reviews
d. carry out checks

The Schools IT Team ensure:

a. they are aware of and follow the school ESafety Policy to carry out their work effectively in line with school policy
b. the school technical infrastructure is secure and is not open to misuse or malicious attack
c. the school meets the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges document
d. there is clear, safe, and managed control of user access to networks and devices
e. they keep up to date with online safety technical information in order to effectively carry out their ESafety role and to inform and update others as relevant
f. the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to (the IT Network Manager) for investigation and action
g. the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person
h. monitoring systems are implemented and regularly updated as agreed in school policies.

5X. Students:

a. are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Agreement and ESafety Policy. This includes when using their own devices and own network during school hours
b. should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

c. can approach their tutor, teacher or any staff member if they or someone they know feels vulnerable when using online technology
d. should understand the importance of adopting good ESsafety practice when using digital technologies out of school and realise that the school's ESafety Policy covers their actions out of school, if related to their membership of the school or other policies including Behaviour Policy and Anti Bullying Policy.

5.xi.Parents and carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

The school will take every opportunity to help parents and carers understand these issues through:

a. publishing the school ESafety Policy on the school website which includes the students' Acceptable Use Agreement
b. publish information about appropriate use of social media relating to posts concerning the school
c. The monthly ESafety newsletter updated shared on the school X account and on the Safeguarding and ESafety section of the website
d. Parents' and carers' Information Evenings, newsletters, website, social media and information about national and local online safety campaigns and literature.

Parents and carers will be encouraged to support the school in:

- reinforcing the ESafety messages provided to students in school
- the use of their children's personal devices in the school.

5.xi Community users

Community users who access school systems as part of the wider school provision will be expected to sign an Acceptable Use Agreement before being provided with access to school systems.

The school encourages the engagement of members of the community who can provide valuable contributions to the ESafety provision and actively seeks to share its knowledge and good practice with other schools and the community.

6. Professional Standards

There is an expectation that required professional standards will be applied to online safety as in other aspects of school life. This includes adherence to the guidance set in this policy, but also through the Staff Code of Conduct and School Handbook.

7. Policy

7.i. Online Safety Policy

The DfE guidance "Keeping Children Safe in Education" states:

"Online safety and the school or college's approach to it should be reflected in the child protection policy" - due to the extensive nature of Esafety, the school wishes to have a separate policy which works alongside the Child Protection Policy.

7.ii. The school ESafety Policy:

a. sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
b. allocates responsibilities for the delivery of the policy
c. is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
d. establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard students in the digital world
e. describes how the school will help prepare students to be safe and responsible users of online technologies
f. establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
g. is supplemented by a series of related acceptable use agreements
h. is made available to staff at induction and through safeguarding training
i. is published on the school website.

8. Acceptable use

The school has defined what it regards as acceptable/unacceptable use and this is shown in the tables below.

8.i. Acceptable use agreements

An Acceptable Use Agreement is a document that outlines a school's expectations on the responsible use of technology by its users. At Whitley Bay High School all users agree to this when they log on to any device. Acceptable Use Agreements are outlined in the appendicies.

8.ii. The ESafety Policy and acceptable use agreements define acceptable use at the school. The acceptable use agreements will be communicated/re-enforced through:

- staff induction and handbook
- splash screens
- communication with parents/carers
- Personal Development Curriculum (including assemblies)
- The school curriculum
- school website
- peer support.

8.iii. The following table is used as guidance for members of the school community on what is Acceptable Use:

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Any illegal activity for example:** • Child sexual abuse imagery • Child sexual abuse/exploitation/grooming • Terrorism • Encouraging or assisting suicide • Offences relating to sexual images i.e., revenge and extreme pornography, sexting • Incitement to and threats of violence • Hate crime • Public order offences - harassment and stalking • Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering When necessary, WBHS will refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					X
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	• Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g., financial /					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission) WBHS will decide whether these should be dealt with internally or by the police. Serious or repeat offences could be reported to the police. Under the Cyber-Prevent agenda the National Crime Agency has a remit to prevent students becoming involved in cyber-crime and harness their activity in positive ways – further information here.					
Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)				X	
	Promotion of any kind of discrimination				X	
	Using school systems to run a private business				X	
	Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				X	
	Infringing copyright or downloading licensed material illegally (such as software, videos, music)				X	
	Submitting work that is not their own. This could be through plagiarism, or artificial intelligence				X	

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X		
	Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

Consideration should be given for the following activities when undertaken for non-educational purposes:	**Staff and other adults**				**Students**			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission/ awareness
Online gaming			x					x
Online shopping/commerce			x				x	
File sharing		x					x	
Social media				x			x	

Messaging/chat			x				x	
Entertainment streaming e.g. Netflix, Disney+			x				x	
Use of video broadcasting, (YouTube only)		X					x	
Mobile phones may be brought to school		X				x		
Use of mobile phones for learning at school		X					x	
Use of mobile phones in social time at school		X				x		
Taking photos on mobile phones/cameras			X				x	
Use of other personal devices, e.g. tablets, gaming devices		X				x		
Use of personal e-mail in school, or on school network/wi-fi		X					x	
Use of school e-mail for personal e-mails	x					x		
Peer to peer networking		x					x	

Installing pirated software on WBHS issued device	x				x			
Use of TOR browsers to access the Dark Web	x				x			
Sharing WBHS data on personal devices and email accounts	x				x			
Use of Artificial Intelligence			X				X	

8.v. When using communication technologies, the school considers the following as good practice:

a. when communicating in a professional capacity, staff should ensure school Office 365 including email accounts are used
b. any digital communication between staff and students or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content. Personal e-mail addresses, text messaging or social media must not be used for these communications
c. staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community
d. users should immediately report to a 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
e. any school social media account must be agreed with the Esafety lead before it is created and any content is posted online. This includes username and password disclosure for monitoring purposes.

9. Reporting and responding

9.i. The 2021 Ofsted "Review of Sexual Abuse in Schools and Colleges" highlighted the need for schools to understand that reporting systems do not always respond to the needs of students. While the report looks specifically at harmful sexual behaviours, schools may wish to address these issues more generally in reviewing their reporting systems. The Ofsted review suggested:

> *"School and college leaders should create a culture where sexual harassment and online sexual abuse are not tolerated, and where they identify issues and intervene early to better protect children and young people. ..In order to do this, they should assume that sexual harassment*

and online sexual abuse are happening in their setting, even when there are no specific reports, and put in place a whole-school approach to address them. This should include:

- *routine record-keeping and analysis of sexual harassment and sexual violence, including online, to identify patterns and intervene early to prevent abuse"*

9.ii. As a result of this, all record keeping at Whitley Bay High School will be in the form of CPOMS, with resulting actions agreed within the Safeguarding Team, with trends being discussed in the half termly meeting.

9.iii. The school will take all reasonable precautions to ensure ESafety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

a. there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies. Reporting will be encouraged in the same way as any safeguarding concern, through the Safeguarding Team. This will be recorded on CPOMS
b. all members of the school community will be made aware of the need to report ESafety issues/incidents
c. reports will be dealt with as soon as is practically possible once they are received
d. the Designated Safeguarding Lead, ESafety Lead and other responsible staff have appropriate skills and training to deal with online safety risks
e. if there is any suspicion that the incident involves any illegal activity or the potential for serious harm (see flowchart and user actions chart in section 9iv), the incident must be escalated through the agreed school safeguarding procedures which is likely to include Police referral. This may include:

I. Non-consensual images
II. Self-generated images (compromising photos of themselves being stored on their device or shared with others)
III. Terrorism/extremism
IV. Hate crime/ Abuse
V. Fraud and extortion
VI. Harassment/stalking
VII. Child Sexual Abuse Material (CSAM)
VIII. Child Sexual Exploitation Grooming
IX. Extreme Pornography
X. Sale of illegal materials/substances o Cyber or hacking offences under the Computer Misuse Act
XI. Copyright theft or piracy

f. any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the local authority. The Headteacher will then follow usual disciplinary procedures if necessary

g. where there is no suspected illegal activity, student devices may be checked using the procedures below:

I. one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported

II. conduct the procedure using a designated device that will not be used by students and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure

III. ensure that the relevant staff 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)

IV. 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 uploaded to CPOMS

V. once this has been completed and fully investigated, the Headteacher 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:

1. internal response or discipline procedures following the Behaviour and Exclusions policies
2. involvement by local authority / MAT (as relevant)
3. Police involvement and/or action.

h. it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively

i. the pastoral team supports students for those reporting or who may be affected by an online safety incident

j. incidents should be logged on CPOMS

k. relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; *Professionals Online Safety Helpline; Reporting Harmful Content; CEOP*

l. If appropriate, those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions

m. learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:

I. the Safeguarding team for consideration of updates to policies or education programmes and to review how effectively the report was dealt with

II. staff, through regular briefings

III. students, through assemblies/lessons

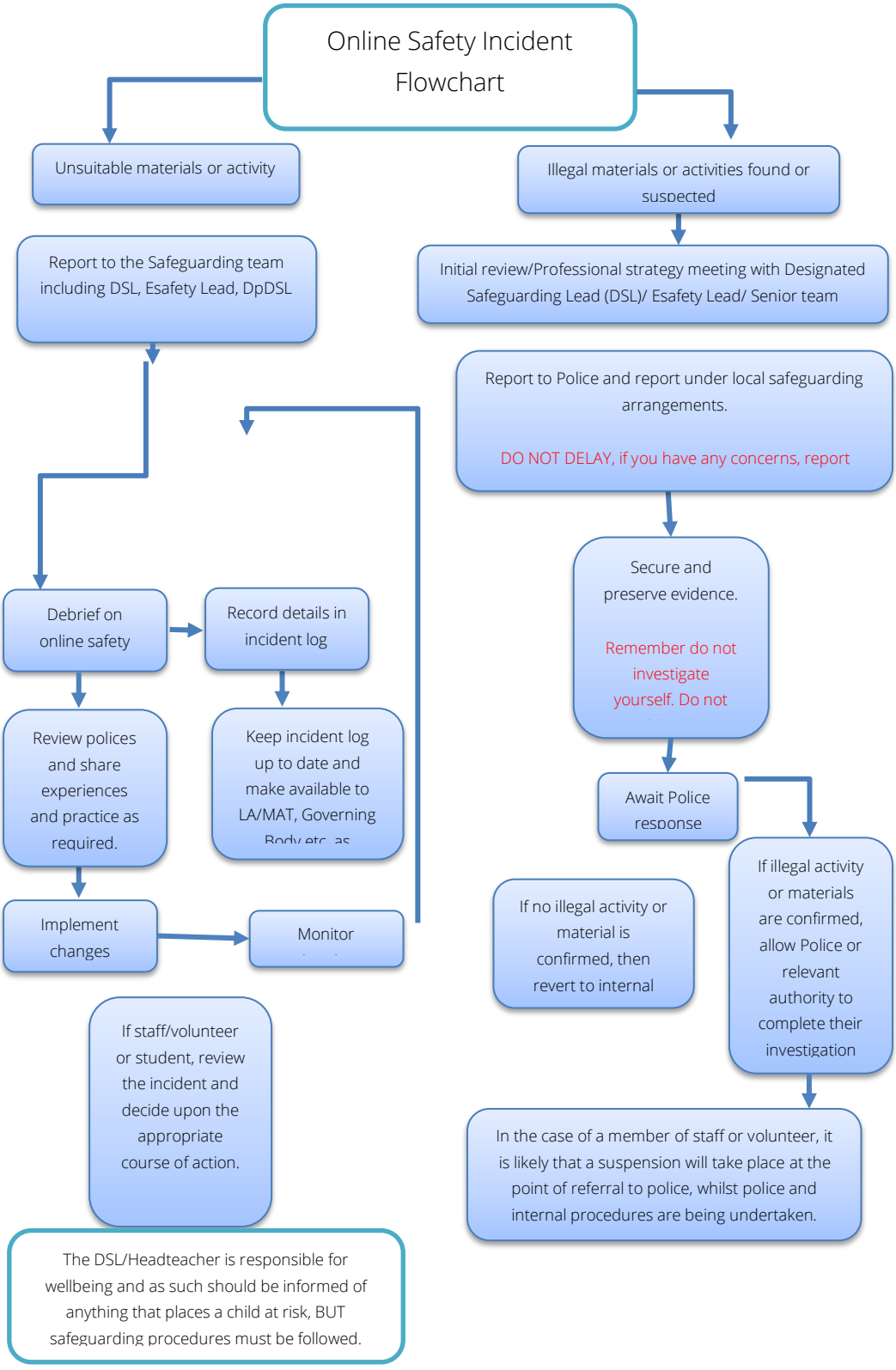
IV. parents/carers, through newsletters, Information Evenings school social media, website.

n. governors, through regular safeguarding updates

o. local authority/external agencies, as relevant (The Ofsted Review into Sexual Abuse in Schools and Colleges suggested "working closely with Local Safeguarding Partnerships in the area

where the school or college is located so they are aware of the range of support available to children and young people who are victims or who perpetrate harmful sexual behaviour".

9.iv. The school will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.



9. v. School actions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

10 . Responding to Actions

10.i. Responding to Student Actions

Incidents	Refer to class teacher/tutor	Refer to Head of Department / Pastoral/Safeguarding	Refer to Esafety Lead Headteacher	Refer to Police/Social Work	Refer to local authority technical support for advice/action	Inform parents/carers (where appropriate)	Remove device/ network/internet access	Issue a warning	Further sanction, in line with behaviour policy
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on User Actions on unsuitable/inappropriate activities).		X	X	X		X			
Attempting to access or accessing the school network, using another user's account (staff or student) or allowing others to access school network by sharing username and passwords			X			X	X	X	X
Corrupting or destroying the data of other users.			X			X	X	X	X
Sending an e-mail, text or message that is regarded as		X	X			X	X	X	X

offensive, harassment or of a bullying nature									
Unauthorised downloading or uploading of files or use of file sharing.		X	X			X	X	X	X
Using proxy sites or other means to subvert the school's filtering system.			X			X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident.		X	X			X			
Deliberately accessing or trying to access offensive or pornographic material.		X	X			X	X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.			X			X	X	X	X
Submitting work that is plagiarised, or created through artificial intelligence.	X	X				X		X	X
Unauthorised use of digital devices (including taking images of staff and students)		X	X			X		X	X
Unauthorised use of online services		X	X			X		X	X
Actions which could bring the school into disrepute or		X	X			X	X	X	X

breach the integrity or the ethos of the school.									
Continued infringements of the above, following previous warnings or sanctions.		X	X			X	X	X	X

10.ii. Responding to Staff Actions

Incidents	Refer to line manager	Refer to Headteacher/ DSL/Esafety Lead	Refer to local authority/MAT/HR	Refer to Police	Refer to LA / Technical Support Staff for action re filtering, etc.	Issue a warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)		**X**	**X**	**X**				
Deliberate actions to breach data protection or network security rules.	x	x	x		x			
Deliberately accessing or trying to access offensive or pornographic material		x	x		x			X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		x	x	x				X
Using proxy sites or other means to subvert the school's filtering system.	x	X						

Unauthorised downloading or uploading of files or file sharing	x	X			x			
Breaching copyright or licensing regulations.	x	x			X			
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.	x	x			x			
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature	x	x						x
Using personal e-mail/social networking/messaging to carry out digital communications with students and parents/carers	x	x						
Inappropriate personal use of the digital technologies e.g. social media / personal e-mail	X	X						X
Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner	X	X						
Actions which could compromise the staff member's professional standing	X	X						X
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.	X	X						X
Failing to report incidents whether caused by deliberate or accidental actions	X	X						X

Continued infringements of the above, following previous warnings or sanctions.		X			X			X

11. ESafety Education Programme

11.i. While regulation and technical solutions are particularly important, their use must be balanced by educating students to take a responsible approach. The education of students in online safety is therefore an essential part of the school's ESafety provision. Students need the help and support of the school to recognise and avoid online safety risks and develop their resilience.

The 2021 Ofsted "Review of Sexual Abuse in Schools and Colleges" highlighted the need for:

> *"a carefully sequenced RSHE curriculum, based on the Department for Education's (DfE's) statutory guidance, that specifically includes sexual harassment and sexual violence, including online. This should include time for open discussion of topics that children and young people tell us they find particularly difficult, such as consent and the sending of 'nudes'.."*

11.ii. ESafety should be a focus in all areas of the curriculum, but particularly in our Personal Development Curriculum. Staff should also reinforce online safety messages across their subject area where appropriate. Our Personal Development Curriculum is broad, relevant and provides age appropriate progression (including a consideration of students capacity to deal with sensitive issues), with opportunities for creative activities and will be provided in the following ways:

a. A planned Personal Development Curriculum which covers ESafety for all year groups developed using the links referenced on the front cover, but particularly Teaching Online Safety in School, and DfE Relationships Education, Relationships and Sex Education and Health Education
b. Lessons are matched to need; are age-related and build on prior learning
c. Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
d. Student need and progress are addressed through effective planning and assessment
e. Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas, for example LEV, Yr 9 IT, IT and Computer Science
f. It incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
g. the programme will be accessible to students at different ages and abilities such as those with additional learning needs or those with English as an additional language
h. students should be helped to understand the need for the Student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school. This will be through the Personal Development programme including assemblies in the first 2 weeks of term

i. staff should act as good role models in their use of digital technologies the internet and mobile devices
j. in lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
k. where students are allowed to freely search the internet, staff should be vigilant in supervising the students and monitoring the content of the websites the young people visit
l. it is accepted that from time to time, for good educational reasons, students may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be logged by the IT Team, with clear reasons for the need
m. the Personal Development Curriculum should be relevant and up to date to ensure the quality of learning and outcomes.

12. Contribution of Students

12.i. The school acknowledges, learns from, and uses the skills and knowledge of students in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for the school community and how this contributes positively to the personal development of young people. Their contribution is recognised through Personal Development student voice and the School Council.

13. Staff/volunteers

13.i. The DfE guidance "Keeping Children Safe in Education" states:

> "All staff should receive appropriate safeguarding and child protection training (including online safety) at induction. The training should be regularly updated. In addition, all staff should receive safeguarding and child protection (including online safety) updates (for example, via email, e-bulletins, and staff meetings), as required, and at least annually, to continue to provide them with relevant skills and knowledge to safeguard children effectively."
>
> "Governing bodies and proprietors should ensure... that safeguarding training for staff, including online safety training, is integrated, aligned and considered as part of the whole school or college safeguarding approach and wider staff training and curriculum planning."
>
> This is incorporated into training and meeting times at WBHS.

13.ii. All staff will receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

a. a programme of formal online safety and data protection training will be made available to all staff. This will be regularly updated and reinforced

b. the training will be an integral part of the school's annual safeguarding and data protection training for all staff
c. all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours
d. the ESafety Lead will receive regular updates through attendance at external training events where appropriate
e. this ESafety Policy and its updates will be presented to and read by all staff.
f. the ESafety Lead will provide advice, guidance and training to individuals as required.

14. Governors

14.i. Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology/online safety/health and safety/safeguarding. This may be offered in several ways such as:

- attendance at training provided by the local authority or other relevant organisation (e.g., North Tyneside Learning Trust)
- participation in school training / information evenings for parents
- participation in training during Full Governors meetings.

14.ii. The ESafety lead and DSL will meet the Safeguarding Governor every half term to make any specific training available.

15. Families

15.i. Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

15.ii. The school will seek to provide information and awareness to parents and carers through:

- this policy
- a monthly Esafety Newsletter posted on X and the school website.
- regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes through X as the issues present themselves.
- regular opportunities for engagement with parents/carers on online safety issues through parent/carer evenings etc
- the students – who are encouraged to pass on to parents the Esafety messages they have learned in lessons.
- letters, newsletters, Office 365 and the school website.
- high profile events and campaigns e.g. Safer Internet Day

- reference to the relevant web sites/publications, e.g. SWGfL; www.saferinternet.org.uk/; www.childnet.com/parents-and-carers (see Appendix for further links/resources).
- Sharing good practice with other schools in clusters and or the local authority.

16. Adults and Agencies

16.i. The school will provide opportunities for local community groups and members of the wider community to gain from the school's online safety knowledge and experience. This may be offered through the following:

a. Adherence to Acceptable Use Agreements
b. School online monitoring (Securus) and filtering (Smoothwall) security systems
c. Online safety messages targeted towards families and relatives
d. Online safety information via the school website and social media for the wider community.

17. Filtering

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible including monitoring and filtering of the network.

The DfE guidance (for England) on filtering and monitoring in "Keeping Children Safe in Education" states:

"It is essential that governing bodies and proprietors ensure that appropriate filtering and monitoring systems are in place ...governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the … risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filtering and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified. The appropriateness of any filtering and monitoring systems are a matter for individual schools and colleges and will be informed in part, by the risk assessment required by the Prevent Duty. To support schools and colleges to meet this duty, the Department for Education has published filtering and monitoring standards…"

The school filtering and monitoring provision is agreed by senior leaders, governors and the IT Service Provider as part of this ESafety Policy which is reviewed annually and updated in response to changes in technology and patterns of online safety incidents/behaviours.

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL, ESafety lead and Network Manager have responsibility for both online safety and a safe technical infrastructure .

Checks on the filtering and monitoring system are carried out by the IT Service Provider (North Tyneside Local Authority) with the involvement of the Network Manager, the ESafety Lead and a

governor, in particular, when a safeguarding risk is identified or there is a change in working practice.

17.2 Filtering

a. The school filtering system is Smoothwall which is monitored by the IT Team. This is reviewed and updated in response to changes in technology and patterns of online safety incidents/behaviours.
b. The school manages access to content across its systems for all users. The filtering provided meets the standards defined in the UK Safer Internet Centre Appropriate filtering.
c. Access to online content and services is managed for all users.
d. Illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated.
e. There are established and effective routes for users to report inappropriate content through the ESafety lead and Safeguarding team.
f. Any filtering changes must be discussed with the IT team and Esafety lead to ensure it is safe to do so.
g. Filtering logs are regularly reviewed and the Safeguarding Team and ESafety lead is alerted to any breaches of the, Acceptable Use Agreement which are then acted upon.
h. Where personal mobile devices have internet access through the school network and wifi, content is managed in ways that are consistent with school policy and practice.
i. Access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.
j. Wi-Fi is monitored and filtered at the same level as the school network.

17.ii. If necessary, the school will seek advice from, and report issues to, the SWGfL Report Harmful Content site.

18. Monitoring

18.i The school has monitoring systems in place to protect the school, systems and users.

a. The school monitors all network use across all its devices and services.
b. Monitoring reports are produced daily and urgently picked up when necessary. When required, they are acted on and outcomes are recorded by any of the Safeguarding Team through CPOMS. All users are aware that the network (and devices) are monitored.
c. There are effective protocols in place to report abuse/misuse as soon as possible to the Esafety Lead and Safeguarding Team. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention. Management of serious safeguarding alerts is consistent with safeguarding policy and practice.

d. Technical monitoring systems are up to date and managed and logs/alerts are regularly reviewed and acted upon.

18.iii The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through the use of the appropriate blend of strategies informed by the school's risk assessment. These may include:

a. physical monitoring (adult supervision in the classroom)
b. internet use is logged, regularly monitored and reviewed
c. filtering logs are regularly analysed and breaches are reported to senior leaders
d. pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention
e. where possible, school technical staff regularly monitor and record the activity of users on the school technical systems
f. use of a third-party assisted monitoring service to review monitoring logs and report issues to school monitoring lead(s).

19. Technical Security

19.i. The school technical systems will be managed in ways that ensure that the school meets recommended technical requirements by the DfE. This includes:

a. Regular reviews and audits of the safety and security of school technical systems
b. Servers, wireless systems and cabling are securely located and physical access restricted
c. Rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud
d. All users having clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually, by the IT team
e. All users (adults and students) having responsibility for the security of their username and password and must not allow other users to access the systems using their log on details. Users must immediately report any suspicion or evidence that there has been a breach of security
f. All school networks and systems will be protected by secure passwords. Passwords must not be shared with anyone. All users will be provided with a username and password by the IT Team who will keep an up-to-date record of users and their usernames
g. The school operating a 2 factor authentication for Office accounts
h. The master account passwords for the school systems are kept in a secure place. Staff are trained to ensure passwords are strong through appropriate length and use of upper and lower case, numbers and characters.
i. The Network Manager being responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied

j. Any incidents, technical or security breaches are to be reported using "Spiceworks", Email, Telephone or in person to the IT Team
k. Servers, Firewalls, Routers and Wireless Systems are protected using complex passwords The school infrastructure and individual workstations are protected by up-to-date endpoint (anti-virus) software
l. an agreed procedure is in place for the provision of temporary access of 'guests', (e.g., trainee teachers, supply teachers, visitors) onto the school systems. This includes temporary accounts, and access to the visitor wifi
m. School devices used outside of school by staff are expected to be used for work purposes
n. Staff are unable to download or install any programme on school devices unless organised with the IT Team
o. School devices do not have access to USB drives unless organised with the IT team. This is in the rare occasion where file sharing is unmanageable
p. personal use of any device on the school network is regulated by Acceptable Use Agreements that a user consents to when using the network
q. Staff are trained to prevent the unauthorised sharing of personal data unless safely encrypted or otherwise secured. The Data Protection Policy helps to control and protect personal data.

20. Mobile technologies

20.i The DfE guidance "Keeping Children Safe in Education" states:

"The school or college should have a clear policy on the use of mobile and smart technology. Amongst other things this will reflect the fact many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children, whilst at school or college, sexually harass, bully, and control others via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share pornography and other harmful content. Schools and colleges should carefully consider how this is managed on their premises and reflect this in their mobile and smart technology policy and their child protection policy.

20.ii.Mobile technology devices may be school owned/provided or personally owned and might include smartphone, tablet, wearable devices, DfE notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school learning platform and other cloud-based services such as e-mail and data storage. All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational

20.iii. Potential Benefits of Mobile technology

Research has highlighted the widespread uptake of mobile technologies amongst adults and children of all ages. Web-based tools and resources have changed the landscape of learning. Students now have at their fingertips unlimited access to digital content, resources, experts, databases and

communities of interest. By effectively maximizing the use of such resources, schools not only have the opportunity to deepen learning, but they can also develop digital literacy, fluency and citizenship in students that will prepare them for the high tech world in which they will live, learn and work. All students and staff have access to professional standard Office 365 which is used in the workplace. Our belief is that we treat our students as emerging adults, and need to educate them how to use their device appropriately, in preparation for the world of work.

20.iii. Our school behaviour policy explains our approach to mobile phone usage in school. This is outlined below:
Students are expected to act responsibly when using mobile phones in school. It is made clear to all students that the same standards of behaviour are expected online as they are with face-to-face interactions (offline), and everyone in our school community should be treated with kindness, respect and dignity. This is done as part of our commitment to Esafety by students consenting to our Acceptable Use Agreement every time they log on to a computer in school, which is further emphasised in the Personal Development Programme and termly assemblies. Inappropriate online behaviour including bullying, child-on-child abuse, the use of inappropriate language, the soliciting and sharing of nude or semi-nude images and videos and sexual harassment, will be addressed in accordance with the same principles as offline behaviour, including following the child protection policy and speaking to the DSL when an incident raises a safeguarding concern.

a) Any cases of cyber bullying, sexting or other inappropriate on-line behaviour will be dealt with appropriately, usually involving parents and the police. A guide to online behaviour and appropriate actions and sanctions is available in the ESafety Policy.
b) During lessons or tutor time students are asked to place mobile phones in their bags (or a box provided), unless they are being used for learning directed by their teacher. Students will be reminded about this at the start of the lesson.
c) Any issues that staff may have with students placing phones away, staff are asked to call for support using the 'purple card' team. A member of the purple card team will come along to try and resolve the situation swiftly so students can get back to learning in their lesson.
d) If a student continues to refuse to place their phone away, their phone will be stored away for safekeeping until lunchtime, or the end of the school day and the student may also be removed from that lesson. Students will not be able to access their phone during this period (but will always have it over lunchtime so they can buy their lunch).
e) For students who have had their phone removed several times parents will be notified and invited in to discuss this. In extreme cases of defiance, a student may be suspended, or have their phone confiscated.

20.iv. The school Acceptable Use Agreements for staff, students, parents, and carers and the Behaviour Policy outline the expectations around the use of mobile technologies whilst on the school and personal network during school hours. The agreement can be found in Appendix A whilst our Behaviour Policy can be accessed on the school website.

20.v. The school allows:

	School devices	**Personal devices**

	School owned for individual use	School owned for multiple users	Authorised device[3]	Student owned	Staff owned	Visitor owned
Allowed in school	**Yes**	**Yes**	**Yes**	Yes	Yes	Yes
Full network access	Yes	Yes	Yes	Yes (through student wifi)	Yes (through staff wifi)	Yes
Internet only						Yes
No network access						Yes

20.vi. The school has provided technical solutions for the safe use of mobile technology whilst on the school wifi for school and personal devices:

a. All school devices are controlled though the use of Mobile Device Management software
b. Appropriate access control is applied to all mobile devices via the downloading of a certificate in order to access the school wifi
c. The school has addressed broadband performance and capacity to ensure that core educational and administrative activities are not negatively affected by the increase in the number of connected devices
d. For all mobile technologies, filtering through a downloadable certificate will be applied to the internet connection and attempts to bypass this are not permitted. Students who use their own network are expected to adhere to the Acceptable Usage Agreement
e. Appropriate exit processes are implemented for devices no longer used at a school location or by an authorised user. These may include; revoking the link between MDM software and the device, removing proxy settings, ensuring no sensitive data is removed from the network, uninstalling school-licenced software etc
f. All school devices are subject to routine monitoring
g. Pro-active monitoring has been implemented to monitor activity when personal devices are permitted
h. All personal devices are restricted through the implementation of technical solutions that provide appropriate levels of network access

i. Personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device in to the school lies with the user (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in school
j. The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home)
k. The school accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network or whilst resolving any connectivity issues
l. The school recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the school. Pass-codes or PINs should be set on personal devices to aid security
m. The school is not responsible for the day to day maintenance or upkeep of the users personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues.

20.v.ii. Users are expected to act responsibly, safely and respectfully in line with current Acceptable Use Agreements, in addition;

a. Devices may not be used in tests or exams
b. Visitors should be provided with information about how and when they are permitted to use mobile technology in line with local safeguarding arrangements
c. Users are responsible for keeping their device up to date through software, security and app updates. The device is virus protected and should not be capable of passing on infections to the network
d. Users are responsible for charging their own devices and for protecting and looking after their devices while in the school
e. DfE school devices are provided to support learning to students who are classified as Disadvantaged, or when supply allows, has requested IT access. It is expected that students will bring devices to the school as required for checking and updates
f. MDM monitoring software is installed on all DfE school devices that are taken home and used by students to ensure the same level of protection as the school network, occurs at home
g. Confiscation and searching (England) - the school has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate
h. The software/apps originally installed by the school must remain on the school owned device in usable condition and be easily accessible at all times. From time to time the school may add software applications for use in a particular lesson. Periodic checks of devices will be made to ensure that users have not removed required apps
i. The school will ensure that devices contain the necessary apps for school work. Apps added by the school will remain the property of the school and will not be accessible to students on authorised devices once they leave the school roll. Any apps bought by the user on their own account will remain theirs
j. Users should be mindful of the age limits for app purchases and use and should ensure they read the terms and conditions before use
k. Users must only photograph people with their permission. Users must only take pictures or videos that are required for a task or activity. All unnecessary images or videos will be deleted immediately

l. As explained in 20.iii, Devices may be used in lessons in accordance with teacher direction
m. Printing from personal devices will not be possible.

21. Social Media

21.i. Social media (e.g. Facebook, X, TikTok, Snapchat, LinkedIn) is a broad term for any kind of online platform which enables people to directly interact with each other. However, some games, for example Minecraft or World of Warcraft and video sharing platforms such as You Tube have social media elements to them.

21.ii. The school recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents/carers and students are actively encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This section aims to encourage the safe use of social media by the school, its staff, parents, carers and children.

21.iii. Social media use is subject to the school's codes of conduct and Acceptable Use Agreements.

This:

a. Applies to all staff and to all online communications which directly or indirectly, represent the school
b. Applies to such online communications posted at any time and from anywhere
c. Encourages the safe and responsible use of social media through training and education
d. Defines the monitoring of public social media activity pertaining to the school.

21.iv. The school respects privacy and understands that staff and students may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.

21.v. Professional communications are those made through official channels, posted on a school account or using the school name. All professional communications are within the scope of this policy.

21.vi. Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.

21.vii. Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

21. Viii Organisational control

Roles & Responsibilities

SLT

a. Facilitating training and guidance on Social Media use.
b. Developing and implementing the Social Media section of the Esafety policy.
c. Taking a lead role in investigating any reported incidents.
d. Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.
e. Receive applications for Social Media accounts.
f. Approve account creation.

Administrator/Moderator

a. Create the account following SLT approval.
b. Store account details, including passwords securely.
c. Be involved in monitoring and contributing to the account.
d. Control the process for managing an account after the lead staff member has left the organisation (closing or transferring). This will involve closing the account, or the Esafety lead meeting with the new account holder in advance of any new post.

Staff

a. Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies.
b. Attending appropriate training.
c. Regularly monitoring, updating and managing content he/she has posted via school accounts.
d. Adding an appropriate disclaimer to personal accounts when naming the school.

21. Ix. Process for creating new accounts

The school community is encouraged to consider if a social media account will help them in their work, e.g. a history department X account, or a "Friends of the school" Facebook page. Anyone wishing to create such an account must discuss with the Esafety lead the following points:

a. The aim of the account
b. The intended audience
c. How the account will be promoted
d. Who will run the account (at least two staff members should be named)
e. Will the account be open or private/closed
f. The intended username and password.

Following consideration by the Esafety lead an application will be approved or rejected. In all cases, the SLT must be satisfied that anyone running a social media account on behalf of the school has read

and understood this section of the Esafety policy and received appropriate guidance. This also applies to anyone who is not directly employed by the school, including volunteers or parents.

21.x. Monitoring

School accounts will be monitored regularly and frequently using Tweet Deck and IT Team checks.

21.xi. Behaviour

a. The school requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.
b. Digital communications by staff must be professional and respectful at all times and in accordance with this policy. Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. School social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school.
c. If a journalist makes contact about posts made using social media staff must contact SLT who may liaise with North Tyneside Local Authority press department before considering whether a reply would be made.
d. Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.
e. The use of social media by staff while at work may be monitored, in line with school policies. The school permits reasonable and appropriate access to private social media sites. However, where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.
f. The school will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies, and may take relevant disciplinary action.

21.xii.Legal considerations

a. Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.
b. Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.

21.xiii. Handling abuse

a. When acting on behalf of the school, users should respond to harmful and / or offensive comments swiftly and with sensitivity.
b. If a conversation turns and becomes offensive or unacceptable, school users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken.
c. If you feel that you or someone else is subject to abuse by colleagues through use of online communications, then this action must be reported following the Whistle Blowing Policy (available on the Staff SharePoint).

21. Xiv. Tone

The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing online content are:

a. Engaging
b. Conversational
c. Informative
d. Professional.

21.xv. Use of images

Students give consent for the taking and sharing of images as part of GDPR data consent at the start of the year. School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

a. Permission to use any photos or video recordings should be sought with the students before taking the video or image. If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.
b. Under no circumstances should staff share or upload student pictures online other than via official school channels.
c. Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Students should be appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published.
d. If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

21.xvi.Personal use

Staff

a. Personal communications are those made via a personal online accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
b. Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
c. Where excessive or inappropriate personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.
d. The school permits reasonable and appropriate access to private social media sites.
e. Staff should ensure safety settings are on the highest level possible to ensure access to their information is controlled. This should include regularly testing of security settings.
f. Staff may consider creating and using accounts under a less identifiable name to protect their privacy and make it more difficult for students to access their content.
g. Inappropriate posts from staff will follow standard disciplinary procedures outlined in the Staff Code of Conduct.

Students

a. Staff are not permitted to follow or engage with current or prior students of the school on any personal social media account. Any exception to this must be discussed with the Esafety lead (for example when a teacher's child is friends with them via social media accounts). Ex students may make attempts to engage with staff social media accounts once they leave school. Staff need to be aware that they may have younger siblings who may access their information via their siblings account.

b. The school's education programme should enable the students to be safe and responsible users of social media.

c. Students are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments will be resolved by the use of the school's Behaviour Policy.

d. Control of student social media use is difficult, as most social media age to use begins at 13, which is the entry age for Year 9 students. Therefore, although the school acknowledges issues with social media use, it is not illegal.

Parents/Carers

a. The school has an active parent/carer education programme which supports the safe and positive use of social media. This includes information on the website and the ESafety newsletter.

b. Parents/Carers are encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's complaints procedures.

21.x.viii. Monitoring posts about the school

- As part of active social media engagement, the school uses Tweet Deck and Google Alerts to monitor the Internet for public postings about the school.
- The school, via social media splash pages, invites parents and members of the community to contact the office to discuss any issues. The school will not engage in online disputes, therefore we urge direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

21xix. General Guidance for Social Media Use

Managing your personal use of Social Media:

a. "Nothing" on social media is truly private

b. Social media can blur the lines between your professional and private life. Don't use the school logo and/or branding on personal accounts

c. Check your settings regularly and test your privacy

d. Keep an eye on your digital footprint

e. Keep your personal information private

f. Regularly review your connections – keep them to those you want to be connected to

g. When posting online consider; Scale, Audience and Permanency of what you post

h. If you want to criticise, do it politely and professionally

i. Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
j. Know how to report a problem.

Managing school social media accounts

The Do's

a. Check with a senior leader before publishing content that may have controversial implications for the school
b. Use a disclaimer when expressing personal views
c. Make it clear who is posting content
d. Use an appropriate and professional tone
e. Be respectful to all parties
f. Ensure you have permission to 'share' other peoples' materials and acknowledge the author
g. Express opinions but do so in a balanced and measured manner
h. Think before responding to comments and, when in doubt, get a second opinion
i. Seek advice and report any mistakes using the school's reporting process
j. Consider turning off tagging people in images where possible
k. Ensure the account is set up securely and the account can be transferred to another approved staff member in the event of the account holder leaving the school.

The Don'ts

a. Don't make comments, post content or link to materials that will bring the school into disrepute
b. Don't publish confidential or commercially sensitive material
c. Don't breach copyright, data protection or other relevant legislation
d. Don't link to, embed or add potentially inappropriate content. Consider the appropriateness of content for any audience of school accounts
e. Don't post derogatory, defamatory, offensive, harassing or discriminatory content
f. Don't use social media to air internal grievances.

22.xx. In the event of any social media issues that the school is unable to resolve support may be sought from the Professionals Online Safety Helpline.

22. Digital and video images

22.i. The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees.

22.ii. The school will inform and educate users about these risks and will implement guidance to reduce the likelihood of the potential for harm:

a. the school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies (found on the SWGfL Safer Remote Learning web pages and in the DfE Safeguarding and remote education)
b. when using digital images, staff will inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images
c. staff/volunteers must be aware of those students whose images must not be taken/published. Any images taken should also ask for consent to further protect these students
d. Personal devices used to take and share public images on social media accounts should be taken, uploaded and deleted as soon as possible
e. in accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other students in the digital/video images
f. care should be taken when sharing digital/video images that students are appropriately dressed
g. students must not take, use, share, publish or distribute images of others without their permission. This includes staff
h. photographs published on the website, or elsewhere that include students will be selected carefully and will comply with ESafety Policy
i. students' full names will not be used anywhere on a website or blog, particularly in association with photographs
j. images will be securely stored in line with the school retention policy.

23. Online Lessons and Video Calls

The development of online lessons has created significant benefits to learning, allowing staff and students to remain learning when off site. However, staff, parents/carers and students need to be aware of the risks associated with online lessons and video calls which are outlined in the section above.

23.i. Staff should follow the guidelines below when hosting an online lesson:

a. Ensure Teams is used as the school's official platform for online lessons.
b. Set Teams up to ensure the teacher is the host and nobody can bypass any lobby.
c. Restrict and monitor access to the team chat – and if not being used for learning turn it off.
d. Ensure the location and background of all students and teacher is plain and non-compromising.
e. Ensure dress is professional and appropriate.

23.ii. Staff should follow the guidelines below when hosting an online call:

a. Where possible use SchoolCloud or Teams as the mechanism for video call. If this is not possible, Zoom should be used.

b. Ensure that any potential participants on the call are made aware of the fact the call may be recorded.

c. Use judgement if a call is not being recorded, but is becoming difficult, to then start the recording.

f. Ensure the location and background is plain and non-compromising.

g. Ensure dress is professional and appropriate.

d. Alert a member of SLT if a difficult conversation is recorded.

e. If the call becomes abusive, end the call promptly and immediately refer to a member of SLT.

f. Remove the conversation in line with the Phone Call Code of Practice after 28 days.

24. Artificial Intelligence (AI)

There is limited guidance available regarding the use of AI in schools. The DfE produced this report Generative artificial intelligence (AI) in education - GOV.UK (www.gov.uk) which also references guidance from the JCQ around malpractice JCQ-AI-Use-in-Assessments-Protecting-the-Integrity-of-Qualifications.pdf. The Government also collected evidence from how schools used AI and published the following document: https://assets.publishing.service.gov.uk/media/65609be50c7ec8000d95bddd/Generative_AI_call_for_evidence_summary_of_responses.pdf. All this information has been used to provide guidance for Whitley Bay HIgh School in section 24 of the ESafety Policy.

Whitley Bay High School will also be conducting research on the use of AI through TLCs (Teaching and Learning Communities) during the spring and summer term. North Tyneside has currently set up a group of leaders to research the use of AI in schools in the authority. This section is therefore due to be updated and refreshed once new guidance becomes available.

24.i. Using the DfE publication, we know that Tools such as ChatGPT and Google Bard can:

- answer questions
- complete written tasks
- respond to prompts in a human-like way

24.ii.Other forms of generative AI can also produce:

- audio
- code
- images
- text

- simulations
- videos

24.iii Generative AI tools are good at quickly:

- analysing, structuring, and writing text
- turning prompts into audio, video and images.

When used appropriately by staff, generative AI has the potential to:

- reduce workload across the education sector
- free up teachers' time, allowing them to focus on delivering excellent teaching
- Produce high quality resources including lessons, schemes of work and lesson resources
- Improve adaptive teaching
- Improve accessibility and inclusion.

When used appropriately by students, generative AI has the potential to:

- provide model examples so students can understand what a good answer looks like
- improve the efficiency of research
- help to produce high quality resources which can be used to prepare students for examinations
- correct imperfections in work
- improve accessibility and inclusion.

24.iv. However, the content produced by generative AI could be:

- inaccurate
- inappropriate
- biased
- taken out of context and without permission
- out of date or unreliable.

24.v. Therefore staff at Whitley Bay High School aim to Explore the use of AI, but:

a. protect personal and special category data in accordance with data protection legislation
b. not allow or cause intellectual property, including students' work, to be used to train generative AI models, without appropriate consent or exemption to copyright
c. review and strengthen their cyber security by referring to the cyber standards – generative AI could increase the sophistication and credibility of attacks

d. ensure that children and young people are not accessing or creating harmful or inappropriate content online, including through generative AI - keeping children safe in education provides schools and colleges with information on:
    I. what they need to do to protect students and students online
    II. how they can limit children's exposure to risks from the school's or college's IT system
e. refer to the filtering and monitoring standard to make sure they have the appropriate systems in place
f. use AI primarily for:
    I. Planning and preparation tasks
    II. Creating educational resources
    III. Administrative tasks
    IV. Research
    V. Creating assessment tasks
g. Until we know more information about AI and assessment, AI will not be used for:
    I. The assessment of student work and the creation of feedback.
h. Understand that AI can produce documentation that is incorrect, therefore ensure any AI generated plans and resources are checked for accuracy.
i. 24.vi. As with the recommendations from the JCQ, students at Whitley Bay High School can not submit work as their own, which has been generated by AI. Students will be educated about the use of AI in their Personal Development Curriculum, which will include how staff will respond if suspected AI malpractice has occurred. This includes:
    I. Notifying the student
    II. Checking AI to see if it has generated the student work
    III. Comparing the submitted work with historical submissions to look at consistency, and realistic progress that could have been made
    IV. Notifying the Head of Department and SLT
    V. Contacting parents
    VI. In extreme cases, it may be necessary to notify the exam board.

25. Online Publishing

25.i The school communicates with parents/carers and the wider community and promotes the school through:

- Public-facing website
- Social media
- Online newsletters
- Esafety newsletters.

25.ii. The school website is managed/hosted by Jump. The school ensures that ESafety policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is least risk to members of the school community, through such publications.

25.iii. Where student work, images or videos are published, their identities are protected, and full names are not published.

25.iv. The school public online publishing provides information about online safety e.g., publishing the schools ESafety Policy and Acceptable Use Agreements; curating latest advice and guidance; news articles etc, creating an online safety page on the school website.

The website includes an online reporting process for parents and the wider community to register issues and concerns to complement the internal reporting process.

26. Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

26.i. The school:

a. has a Data Protection Policy
b. implements the data protection principles and can demonstrate that it does so
c. has paid the appropriate fee to the Information Commissioner's Office (ICO)
d. has appointed an appropriate Data Protection Officer (DPO) who has effective understanding of data protection law and is free from any conflict of interest
e. has a 'Record of Processing Activities' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it
f. the Record of Processing Activities lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis is listed
g. has an 'information asset register' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it
h. information asset register lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis will have also been listed
i. will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. The school 'retention schedule" supports this
j. data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
k. provides staff, parents, volunteers, teenagers, and older children with information about how the school looks after their data and what their rights are in a clear Privacy Notice (see Privacy Notice section in the appendix)

l. has procedures in place to deal with the individual rights of the data subject, e.g. one of the dozen rights applicable is that of Subject Access which enables an individual to see/have a copy of the personal data held about them
m. carries out Data Protection Impact Assessments (DPIA) where necessary e.g. to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier
n. has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors
o. understands how to share data lawfully and safely with other relevant data controllers
p. has clear and understood policies and routines for the deletion and disposal of data
q. reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents
r. has a Freedom of Information Policy which sets out how it will deal with FOI requests
s. provides data protection training for all staff at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.

26.ii. When personal data is stored on any mobile device or removable media the:

a. data will be encrypted, and password protected
b. device will be password protected
c. device will be protected by up-to-date endpoint (anti-virus) software
d. data will be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

26.iii. Staff must ensure that they:

a. at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
b. can recognise a possible breach, understand the need for urgency and know who to report it to within the school
c. can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to in the school
d. only use encrypted data storage for personal data
e. will not transfer any school personal data to personal devices.
f. use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data

g. transfer data using encryption, a secure email account (where appropriate), and secure password protected devices.

27. Outcomes

The impact of the ESafety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, students; parents/carers and is reported to relevant safeguarding groups:

a. there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., ESafety education, awareness, and training
b. there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and Governors
c. parents/carers are informed of patterns of ESafety incidents as part of the school's online safety awareness raising
d. ESafety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate
e. the evidence of impact is shared with other schools, agencies and LAs to help ensure the development of a consistent and effective local ESafety strategy.

Appendix

Copies of the more detailed template policies and agreements, contained in the appendix, can be found in the links and resources section of the relevant aspects in the 360safe self-review tool and online on the SWGfL website. The appendices are as follows:

- A – Pupil Acceptable Use Agreement
- B – Staff Acceptable Use Agreement

Appendix A Student Acceptable Use Agreement

School policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe access to these digital technologies.

This acceptable use agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the *students* to agree to be responsible users.

Acceptable Use Agreement

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

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it
- I will be aware of "stranger danger", when I am communicating on-line
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school's systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work
- I will not use the school's systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so
- I will act as I expect others to act toward me

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions
- I will not take or distribute images of anyone without their permission. This includes staff and students.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will follow the school's Behaviour Policy and only use my own personal devices (mobile phones) in school if I have permission from the teacher to do. My device will remain in my bag unless asked to use it. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials
- I will immediately report any damage or faults involving equipment or software, however this may have happened
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings
- I will only use my device for social reasons during break and lunch.

When using the internet for research or recreation, I recognise that:

- I should 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 try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be online-bullying, use of images or personal information)
- I understand that if I fail to comply with this acceptable use agreement, I may be subject to disciplinary action in line with the Behaviour Policy. This could include confiscation of personal devices, loss of access to the school network/internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please click the countersignature box to provide an electronic signature to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Appendix B Staff /Community/Volunteer Acceptable Use Policy Agreement Template

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This acceptable use policy is intended to ensure:

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

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the school digital technology and communications systems
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school Esafety and Staff Code of Conduct Policy
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's guidance on the use of digital/video images. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured
- I will only use social networking sites in school in accordance with the school's social media guidance (via Esafety Policy)
- I will only communicate with students and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses
- I will not use personal email addresses on the school's ICT systems
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in agreement with the Network Manager.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage

- I understand that the Data Protection Policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the online systems in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this acceptable use policy applies not only to my work and use of school's digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could be a warning, a suspension, referral to Governors/Trustees and/or the Local Authority and in the event of illegal activities the involvement of the police.

Please click the countersignature box to provide an electronic signature to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.