E SAFETY POLICY

Date	January 2026 This policy will be reviewed annually Statutory Policy
Review Date	January 2027
Author	Andy Sherlaw, WBHS
Approved by	Finance & Premises Committee
Full Governing Body Approval	5 February 2026

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 2025 Keeping children safe in education 2025
- 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
- Generative AI: product safety standards
- JCQ-AI-Use-in-Assessments-Protecting-the-Integrity-of-Qualifications.pdf. T
- Meetings Digital and Technology Standards in School Meeting digital and technology standards in schools and colleges - Cyber security standards for schools and colleges - Guidance - GOV.UK
- Searching, Screening and Confiscation (publishing.service.gov.uk)
- Sharing of Nudes and Semi Nudes and How to Respond to an Incident Sharing nudes and semi-nudes: how to respond to an incident (overview) (updated March 2024) - GOV.UK
- SWGfl: https://swgfl.org.uk/resources/online-safety-policy-templates/
- Teaching Online Safety in School January 2023: 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
- The Safe and Effective Use of AI in Education: https://assets.publishing.service.gov.uk/media/6842e04ee5a089417c8060c5/Leadership_Toolkit_-_Transcript.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

Contents Page

1. Scope of the Online Safety Policy	1
2. Policy development, monitoring and review	2
3. Schedule for development, monitoring and review	2
4. Process for monitoring the impact of the ESafety Policy	3
5. Policy and leadership	4
6. Professional Standards	11
7. Policy	12
8. Acceptable use	13
9. Reporting and responding	18
10 . Responding to Actions (students and staff)	22
11. ESafety Education Programme	26
12. Contribution of Students	28
13. Staff/volunteers	28
14. Governors	29
15. Families	29
16. Adults and Agencies	30
17. Filtering	30

18. Monitoring	32
19. Technical Security	33
20. Mobile Technologies	35
21. Social Media	39
22. Digital and Video Images	45
23. Online Lessons and Video Calls	47
24. Artificial Intelligence	47
25. Online Publishing	54
26. Data Protection	54
27. Cyber Security	56
28. Outcomes	56
Appendix A Student Acceptable Use Agreement	58
Appendix B Staff (visitor/community/volunteer) Acceptable Use Agreement	61

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.

It is essential that children are safeguarded from potentially harmful and inappropriate online material. Our whole school approach to **online safety** empowers us to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

Our Governing body ensures **online safety** is a running and interrelated theme whilst devising and implementing our whole school approach to safeguarding and related policies and procedures. This includes considering how **online safety** is reflected in relevant policies, the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead (and deputies) and any parental engagement"

The DfE Keeping Children Safe in Education guidance recommends:

Reviewing online safety *-Technology, and risks and harms related to it, evolve, and change rapidly. Schools and colleges should consider carrying out an annual review of their approach to online safety, supported by an annual risk assessment that considers and reflects the risks their children face.*

The DfE Keeping Children Safe in Education guidance also suggests that:

> *The breadth of issues classified within online and ESafety is considerable and ever evolving, but can be categorised into four areas of risk:*
>
> ***content:*** *being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.*
>
> ***contact:*** *being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.*
>
> ***conduct:*** *online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and nonconsensual sharing of*

nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and

commerce: *risks such as online gambling, inappropriate advertising, phishing and or financial scams.*

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 ESafety policy has been developed by the Finance and Premises Governing Body working group made up of:

- Headteacher
- ESafety Leader (Deputy Headteacher and DpDSL)
- Staff including GDPR Lead
- Governors of the Finance and Premises committee

3. Schedule for development, monitoring and review

3.i. This ESafety Policy was approved by the Finance and Premises *governing body on:*	*22.1.25*
3.ii. The implementation of this ESafety Policy will be monitored by:	ESafety Deputy Headteacher / Network Manager / Finance and Premises Committee/ Senior Leadership/ and IT 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 and Risk Assessment to be reviewed annually.*
3.iv. The *governing body* will receive updates on the implementation of the ESafety Policy generated by the	As part of Safeguarding updates in Full Governors when necessary.

monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	As part of the Safeguarding Governors school visits
3.v The ESafety 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 2026*
3vi. Should serious ESafety 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)
- Student voice via the School Council
- Parents / carer voice
- Low level staffing concerns recorded in Staff Safe
- Staff voice

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 ESafety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for ESafety. They are closely supported by the DSL and 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 ESafety 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 and updates from the ESafety Lead.
f. The headteacher, ESafety Lead, and Safeguarding Team (including DSL) will work with the responsible Governor and IT service providers in all aspects of filtering and monitoring.

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"

"Governing bodies and proprietors should ensure an appropriate senior member of staff, from the school or college leadership team, is appointed to the role of designated safeguarding lead. The designated safeguarding lead should take lead responsibility for safeguarding and

[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.

child protection (including online safety and understanding the filtering and monitoring systems and processes in place)"

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".

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:

- regular meetings with the Safeguarding lead (DSL)
- regularly receiving (collated and anonymised) reports of online safety incidents
- checking that provision outlined in the ESafety Policy (e.g. online safety education provision and staff training is taking place as intended)
- Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually in-line with the DfE Filtering and Monitoring Standards
- reporting any ESafety issues alongside the ESafety Lead to Full Governors *meetings held every term.*
- Receiving (at least) basic cyber-security training to enable the governors to check that the school meets the DfE Cyber-Security Standards

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. DSL and ESafety Lead

Designated Safety Lead (DSL)
Keeping Children Safe in Education states that:

> *"The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place). This should be explicit in the role holder's job description."*
>
> *They (the DSL) "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"*
>
> *They (the DSL) "*can recognise the additional risks that children with special educational needs and disabilities (SEND) face online, for example, from bullying, grooming and radicalisation and are confident they have the capability to support children with SEND to stay safe online"

At Whitley Bay High School, an Esafety Lead is appointed to support the DSL.

The DSL will continue to:

a. hold the lead responsibility for online safety, within their safeguarding role.
b. Receive relevant and regularly updated training in online safety to enable them to understand the 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
c. meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out
d. attend relevant governing body meetings/groups
e. report regularly to headteacher/senior leadership team
f. be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
g. liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety).

The Esafety Lead will:

h. lead online developments and updates in the half termly Safeguarding Team meeting
a. work closely on a day-to-day basis with the Designated Safeguarding Lead (DSL)
b. take day-to-day responsibility for ESafety issues, being aware of the potential for serious child protection concerns, ensuring these are logged to inform future online safety developments
c. have a leading role in establishing and reviewing the school ESafety policy
d. work with the Personal Development Lead to promote an awareness of and commitment to online and ESafety education across the curriculum and beyond
e. promote an awareness of and commitment to ESafety education across the school and beyond
f. liaise with Personal Development Lead to ensure that the ESafety 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 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. liaise with the local authority when relevant
o. Check the IT team are doing regular checks of the monitoring and filtering systems
p. Ensure the school adheres to the minimum standards for cyber security in schools
q. receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined In Keeping Children Safe in Education:
    i. Content
    ii. Contact
    iii. Conduct
    iv. commerce

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 and online behaviour.

5.v. 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.a. 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 and sharing of nude images
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 and 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 accepted the Staff Acceptable Use Agreement (AUA) when they log onto their computer
d. they follow all relevant guidance and legislation including, for example, Keeping Children Safe in Education and UK GDPR regulations
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. Where staff use AI to assist this communication, they should only use Microsoft CoPilot to comply with organisational security and oversight requirements
f. 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
g. online safety issues are embedded in all aspects of the curriculum and other activities
h. 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, including plagiarism through use of AI and uphold copyright regulations
i. 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
j. 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

k. 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
l. have a vigilant and prompt approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc in line with any child protection concern
m. they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of personal devices and social media. Staff will receive ESafety 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
n. they adhere to the school's technical security policy, with regard to the use of devices, systems and passwords and have an understanding of basic cybersecurity
o. they have a general understanding of how the learners in their care use digital technologies out of school, in order to be aware of ESafety issues that may develop from the use of those technologies
p. they are aware of the benefits and risks of the use of Artificial Intelligence (AI) services in school, being transparent in how they use these services, prioritising human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans, fact-checked and critically evaluated.

5. viii 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"

5 vix Schools Network manager and technical staff in the 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 IT team and Local Authroity are responsible for ensuring that:

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 and the DfE Cyber Security minimum standards.
d. The school minimises the risk of a cyber attack by implementing the Cyber Response Plan which includes strong and regularly updated passwords and regular training opportunities for all stakeholders
e. there is clear, safe, and managed control of user access to networks and devices
f. 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
g. the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to the IT Network Manager or ESafety Lead for investigation and action
h. the filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person
i. 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.

e. should avoid plagiarism and uphold copyright regulations, taking care when using Artificial Intelligence (AI) services to protect the intellectual property of themselves and others and checking the accuracy of content accessed through AI services.

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. publishing information about appropriate use of social media relating to posts concerning the school
C. seeking their permissions concerning digital images, cloud services etc
d. The monthly ESafety newsletter updated shared on the school Instagram account and on the Safeguarding and ESafety section of the website
e. 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:

f. reinforcing the ESafety messages provided to students in school
g. the safe and responsible use of their children's personal devices in the school (where this is allowed)

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 i.e.

a. there is a consistent emphasis on the central importance of literacy, numeracy, digital competence and digital resilience. Learners will be supported in gaining skills across all areas of the curriculum and every opportunity will be taken to extend learners' skills and competence
b. there is a willingness to develop and apply new techniques to suit the purposes of intended learning in a structured and considered approach and to learn from the experience, while taking care to avoid risks that may be attached to the adoption of developing technologies e.g. Artificial Intelligence (AI) tools.

c. Staff are able to reflect on their practice, individually and collectively, against agreed standards of effective practice and affirm and celebrate their successes
d. policies and protocols are in place for the use of online communication technology between the staff and other members of the school and wider community, using officially sanctioned school mechanisms.
e. Where Generative AI is used to monitor staff communications, it will be balanced with respect for privacy and transparency about what is being monitored and why.

Professional standards also includes adherence to the guidance set in this policy, but also through the Staff Code of Conduct and School Handbook.

7. Policy

7.i. ESafety 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 appendices.

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 during Information Evenings and through the school Instagram account and monthly ESafety newsletter
- 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	**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 and sharing nudes • Incitement to and threats of violence • Hate crime • Public order offences - harassment and stalking					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
contain or relate to:	• 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					
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 / 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					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	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/monitoring 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 and infringing copyright and intellectual property. This could be through plagiarism, or artificial intelligence				X	
	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. If AI is used to support these communications, Microsoft CoPilot is the only AI the school permits use of.
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. Staff should be aware of the increasing number of Freedom of Information requests, including subject access requests (SARs) which will result in publication of associated documents which include emails.
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 one of the Safeguarding Team or SLT 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. Username and passwords will also be held on a separate password protected document.

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 for students, and StaffSafe for staff, with resulting actions agreed within the Safeguarding Team, with trends being discussed in the half termly meetings.

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
XII. Cyber or hacking offences under the Computer Misuse Act
XIII. Illegal use of AI (usually associated in conjunction with one of the incidents above)

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 AI is used to support monitoring and incident reporting, human oversight is maintained to interpret nuances and context that AI might miss
h. 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.

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

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

k. incidents should be logged on CPOMS

l. 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*

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

n. 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

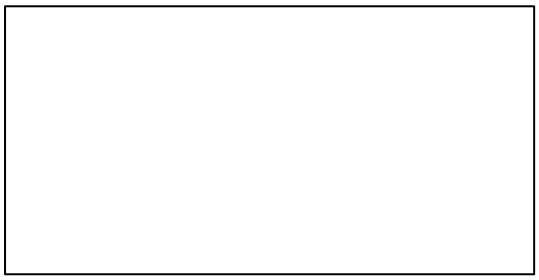
II. staff, through regular briefings and training

III. students, through assemblies/lessons

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

V. governors, through regular safeguarding updates

VI. local authority/external agencies, as relevant 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. 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 offensive, harassment or of a bullying nature		X	X			X	X	X	X

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 AI generated. Breaching copyright/ intellectual property or licensing regulations (including through the use of AI systems)	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 breach the integrity or the ethos of the school.		X	X			X	X	X	X
Deliberately responding to phishing attacks or any actions that make the school more vulnerable to cyber attacks.			X			X	X	X	X
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 and cyber security rules as outlined in the Cyber Response Plan	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 / non approved AI whilst using school associated data	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
Careless use of technology which causes a data protection breach	X	X						
Careless use of digital technologies which causes the school to be at greater risk of a cyber attack	X	X						
Failing to report incidents whether caused by deliberate or accidental actions	X	X						X
Breaching copyright/ intellectual property or licensing regulations (including through the use of AI systems)	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'.."*

Keeping Children Safe in Education states:

"Governing bodies and proprietors should ensure online safety is a running and interrelated theme whilst devising and implementing their whole school or college approach to safeguarding and related policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum …"

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. Lessons and the Personal Development Curriculum can also be personalised when necessary to meet the needs of vulnerable students e.g. for victims of abuse and SEND students
c. Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
d. learners should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information (including where the information is gained from Artificial Intelligence services which could contain bias and ethical considerations)
e. learners should be taught to acknowledge the source of information used and to respect copyright / intellectual property when using material accessed on the internet and particularly through the use of Artificial Intelligence services
f. Student need and progress are addressed through effective planning and assessment.
g. 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
h. It incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
i. 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
j. 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
k. staff should act as good role models in their use of digital technologies the internet and mobile devices

l. In lessons where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites / tools (including AI systems) the learners visit
m. 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
n. 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
o. 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, ESafety and AI 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, ESafety 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, data protection and cyber-security training for all staff

c. all new staff will receive online and ESafety 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 and by reviewing guidance documents released by relevant organisations
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 and ESafety training/awareness sessions, with particular importance for the Safeguarding Governor. This could include:

- 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.
- Cyber-security training (at least at a basic level)
- Training to allow the governor to understand the school's filtering and monitoring provision, in order that they can participate in the required checks and review.

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

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 Instagram and the school website.
- regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes through Instagram 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

The DfE Technical Standards for Schools and Colleges states:

“Schools and colleges have a statutory responsibility to keep children and young people safe online as well as offline. Governing bodies and proprietors should make sure their school or college has appropriate filtering and monitoring systems in place, as detailed in the statutory guidance, Keeping children safe in education.

Filtering is preventative. It refers to solutions that protect users from accessing illegal, inappropriate and potentially harmful content online. It does this by identifying and blocking specific web links and web content in the form of text, images, audio and video

These standards help school and college leaders, designated safeguarding leads and IT support understand how to work together to make sure they can effectively safeguard their students and staff.”

The ESafety Lead and Safeguarding Governor, are responsible for ensuring filtering standards are met.

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 DfE Filtering standards for schools and colleges and the guidance provided 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, recognising that no system can be 100% effective. Any student or staff concerns are reported

to the ESafety Lead and Safeguarding team. These are acted upon in a timely manner, within clearly established procedures

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. There are regular checks of the effectiveness of the filtering systems. Checks are undertaken across a range of devices at least termly and the results recorded and analysed to inform and improve provision. The ESafety Lead., DSL and Governor are involved in the process and aware of the findings.
i. Devices that are provided by the school have school-based filtering applied irrespective of their location.
j. 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.
k. 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.
l. 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 Service and other relevant agencies.

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

18. Monitoring

The DfE Technical Standards for Schools and Colleges states:

"Monitoring is reactive. It refers to solutions that monitor what users are doing on devices and, in some cases, records this activity. Monitoring can be manual, for example, teachers viewing screens as they walk around a classroom. Technical monitoring solutions rely on software applied to a device that views a user's activity. Reports or alerts are generated based on illegal, inappropriate, or potentially harmful activities, including bullying. Monitoring solutions do not block users from seeing or doing anything."

18.i 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 outlined below.

18.ii **The school has monitoring systems in place, agreed by senior leaders and technical staff, to protect the school, systems and users. Whitley Bay High School uses Securus as its main monitoring software. In addition:**

- The school monitors all network use across all its devices and services.

- 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.
- 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.
- Technical monitoring systems are up to date and managed and logs/alerts are regularly reviewed and acted upon.
- Devices that are provided by the school have school-based monitoring applied irrespective of their location.
- Monitoring enables alerts to be matched to users and devices.
- Staff are encouraged to be vigilant in their physical monitoring of IT use in lessons and throughout school. Staff are trained to adopt a 'curious not furious' approach to ensure any ESafety issue (including new apps students discover in their own time) can be addressed.
- *AI supported monitoring software is currently unavailable. Therefore, any AI use in school must be agreed with the ESafety lead with the purpose and scope of its intention clearly communicated. Staff who request this must be vigilant within the lesson using frequent close proximity monitoring and Veon software to minimise any risk.*
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.

The monitoring provision is reviewed at least once every academic year and updated in response to changes in technology and patterns of online safety incidents and behaviours. The review should be conducted by the ESafety Lead, the DSL, technical staff and the Safeguarding Governor. The results of the review will be recorded and reported as relevant.

19. Technical Security

19.i The school technical systems will be managed in ways that ensure that the school meets recommended standards in the DfE Technical Standards for Schools and Colleges. This includes:

a. Responsibility for technical security resides with SLT who may delegate activities to identified roles.
b. A documented access control model is in place, clearly defining access rights to school systems and devices. This is reviewed annually. All users (staff and learners) have 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. This is part of the school's Cyber Response Plan.
c. password policy and procedures are implemented and are consistent with guidance from the National Cyber Security Centre
d. all school networks, devices and system will be protected by secure passwords.
e. the administrator passwords for school systems are kept in a secure place, e.g. school safe.

f. there is a risk-based approach to the allocation of learner usernames and passwords. Students are guided how to have secure and strong passwords through the Personal Development Curriculum.
g. Regular reviews and audits of the safety and security of school technical systems
h. Servers, wireless systems and cabling are securely located and physical access restricted
i. Rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud
j. 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. The security of usernames and passwords must not allow other users to access the systems using their log on details.
k. 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
l. The school operating a 2 factor authentication for Office accounts
m. 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.
n. 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
o. All users must immediately report any suspicion or evidence that there has been a breach of security to a member of staff for students or a member of the Safeguarding Team for staff. Any incidents, technical or security breaches can also be reported using “Spiceworks”, Email, Telephone or in person to the IT Team
p. 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
q. servers, wireless systems and cabling being securely located with physical access restricted
r. 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
s. School devices used outside of school by staff and students are expected to be used for work purposes which is regulated by an acceptable use statement that a user consents to when the device is allocated to them. This includes responsibility for the device being theirs, and that family use should be regulated.
t. Staff are unable to download or install any programme on school devices unless organised with the IT Team
u. 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. Removable media is not permitted unless approved by the SLT/IT service provider
v. personal use of any device on the school network is regulated by Acceptable Use Agreements that a user consents to when using the network

w. Systems are in place that prevent the unauthorised sharing of personal / sensitive data unless safely encrypted or otherwise secured. 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.
x. Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date endpoint software.
y. There are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud,
z. a system in place for users to report any actual/potential technical incident/security breach to the Safeguarding or IT team
aa. mobile device security and management procedures which are in place and follow the same security procedures as any device on site and on the network and wifi following the Acceptable Use Agreement.
bb. Staff can only use Microsoft CoPilot AI system when inputting sensitive information, such as personal data, internal documents or strategic plans, unless a request has been made to use alternative software which has been explicitly vetted for that purpose. Staff must always recognise and safeguard sensitive data and access permission from the ESafety Lead for any alternative to Microsoft CoPilot for these uses.
cc. Dual-factor authentication is used for sensitive data or access outside of a trusted network
dd. Where AI services are used for technical security, their effectiveness is regularly reviewed, updated and monitored for vulnerabilities.
ee. Where AI services are used, the school will work with suppliers to understand how these services are trained and will regularly review flagged incidents to ensure equality for all users e.g. avoiding bias

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 maximising 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[2]	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 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

All schools and local authorities have a duty of care to provide a safe learning environment for learners and staff. Schools could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, bully online, discriminate on the grounds of sex, race, or disability or who defame a third party may render the school liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

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
e. Ensure social media use is not excessive and does not interfere with relevant duties.

21. Ix. Process for creating new accounts

The school has decided to have one official social media account which is Instagram. The only other social media account is a sixth form TikTok. Anyone wishing to create a different school associated account must discuss with the ESafety lead:

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. The school used to operate several X accounts but have consolidated public posts through a smaller number of social media accounts. Therefore, it is highly likely that new requests will be rejected. In all cases, 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

The school has one school Instagram account which is monitored and ran by two staff members including the ESafety lead. The Sixth Form TikTok account is monitored by the Director of Sixth Form. Any social media account must submit their username and password to the IT team for it to be regularly monitored by them as an additional safety mechanism.

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 ESafety 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 regularly checks the social media and uses 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.
k. Consider the Do's and Don'ts from the section below.

Managing and Posting on the 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
g. Don't use AI inappropriately to publish on social media.

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. staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images. 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.
k. learners' work can only be published with the permission of the learner, unless shared anonymously

22.iii. The school utilises surveillance cameras to facilitate two key aims: 1) Ensuring the safety and security of students, staff, and visitors by monitoring gated entry and exit points; 2) To deter acts of anti-social behaviour, vandalism and criminal behaviour in potentially vulnerable areas of the school and to assist with investigations should they occur. The school implements and obides by a Code of Practice governing its use of surveillance cameras and a copy of this is available of the GDPR section of our web site.

22.iv The school also has cameras installed in its food delivery kiosks for the purposes of a biometric recognition system for payment and queue management. Further information on the scope and functions of this system are available from our DPO.

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 Government has many pilot research AI projects occurring now, which will influence this policy in the future. The current DfE guidance was updated in January 2025 Generative artificial intelligence (AI) in education - GOV.UK (www.gov.uk) alongside a new publication Generative AI: Product Safety Expectations to help provide schools with a framework to decide which AI products are safe and effective to use for students and teachers. Additionally, there is 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 has conducted its own research on the use of AI through TLCs (Teaching and Learning Communities) during the spring and summer term of 2024. We are also part of a North Tyneside group of leaders who delivered a conference of the use of AI in schools in the authority. This will continue this academic year. The use of AI to reduce workload for all teachers is currently being led by the training team, and for support staff by the IT team. The advancements in use of AI could be faster than the annual renewal of this policy, therefore the school will always attempt to adhere to the guidance set by the DfE.

Whitley Bay High School will comply with all relevant legislation and guidance, with reference to guidance contained in Keeping Children Safe in Education and UK GDPR

24.i. Generative AI is one type of AI. It refers to technology that can be used to create new content based on large volumes of data that models have been trained on a variety of sources.

ChatGPT, Microsoft Copilot and Google Gemini are generative AI tools, built on large language models (LLMs). LLMs are a category of foundation models trained on large amounts of data, enabling them to understand and generate human-like content. AI can:

- answer questions
- complete written tasks
- Generate images, text or code
- respond to prompts in a human-like way

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

- audio
- simulations
- videos

24.iii AI is the defining technology of our age, and it is evolving at incredible speed. This technology has the potential to benefit the economy and meet societal challenges. This is not new, and we already use AI in everyday life for:

- email spam filtering
- media recommendation systems
- navigation apps
- online chatbots

Advances in technology mean that we can now use these tools to produce AI-generated content. This creates opportunities and challenges for the education sector.

Generative AI tools are good at quickly:

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

The DfE in the Generative AI Product Safety Standards publication have recognised that AI can be used for:

1. **Content creation and delivery**: tools that generate and deliver instructional materials such as lesson plans, presentations, and educational videos, often tailored to a specific subject or topic
2. **Personalised learning and accessibility**: tools designed to create customised learning pathways, adaptive content, and accessible formats for all learners, especially those with special educational needs
3. **Assessment and analytics**: tools that automate the marking of student work, provide detailed performance analytics, and offer personalised feedback to both learners and teachers
4. **Digital assistant**: AI-powered conversational agents, such as personal tutors and chatbots, that provide on-demand support, answer questions, and guide learners through learning tasks
5. **Research and writing aid**: tools that help learners with tasks like topic ideation, summarising research papers, and ensuring proper citation and plagiarism checks
6. **Learner engagement and interaction**: tools that promote active learning, collaborative projects, and meaningful interaction with both peers and AI systems in a safe, moderated environment
7. **Administrative and management**: tools that support school leaders and teachers with administrative tasks, including parent communication, report generation, and ensuring compliance with school policies and DfE guidance
8. **Other**: edtech developers and suppliers should specify if their product does not fall into one of the previous use case categories and provide a clear statement of purpose and use case

Additional to this, 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
- Interact with the student to help revise key topics and concepts
- improve accessibility and inclusion

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

- inaccurate
- inappropriate or unsafe
- biased
- taken out of context
- taken without permission (intellectual property infringement)
- out of date or unreliable
- low quality

This is because generative AI:

- returns results based on its training dataset, which may not be specific to our curriculum
- stores and learns from input data – any data entered should not contain information that could allow an individual to be identified
- may not provide results that are comparable with a human-designed resource developed in the context of our curriculum
- can generate believable content, including credible scam emails
- can provide instructions for illegal or harmful activities
- can produce nonsensical, inaccurate or false information presented as fact, known as hallucination

Consequently, until more work is conducted on the safety aspects of student facing AI, which includes monitoring and filtering systems, we cannot permit student use of AI in school on the student network. This is because generative AI produces original products which could be unsafe for students depending on the prompt and policy of the AI type.

When students are introduced to using AI, any AI product that is used must comply with the DfE Product and Safety Expectations. Students will be also educated on that AI may produce biased,

24.v. Staff at Whitley Bay High School use AI for teaching and learning and also administration tasks. When using AI apps staff must consider data privacy and intellectual property outlined below.

Data privacy
It is important to be aware of the data privacy implications when using generative AI tools

Personal data must be protected in accordance with data protection legislation. Personal data should not be used in generative AI tools. If it is strictly necessary to use personal data in generative AI tools, Microsoft Copilot is the only AI that can be used for Whitley Bay High School data. This is because it complies with:

- data protection legislation
- data privacy policies

Whitley Bay High School will:

- be open and transparent where consideration is being given to the use of automated decision-making and profiling – this includes when we develop their own in-house AI tools, such as AI chatbots or AI digital assistants
- ensure the data subjects (pupils and parents or legal guardians) understand that their personal data is being processed using AI tools

Intellectual property

It is important to be aware of the intellectual property (IP) implications when using generative AI tools

Materials protected by copyright can only be used to train AI if there is permission from the copyright holder, or a statutory exception applies.

Materials created by pupils and teachers may well be copyright material, assuming the statutory standard for what comprises copyright material is satisfied. This standard is generally considered to be low and does not factor in the quality of the work produced.
Copyright law is distinct from data protection law, so any consents or data processing agreements for personal data are separate from issues of compliance with copyright law.
Many free-to-access generative AI tools will use the inputs submitted by users to further train and refine their models. Some tools, largely paid tools, allow users to opt out of inputs being used to train the models.

Examples of what may be deemed original creative work include:

- essays, homework or any other materials written or drawn by a student – it is unlikely that multiple-choice questions responses will constitute copyright work
- lesson plans created by a teacher
- prompts entered into generative AI tools

Permission to use

Schools and colleges must not allow or cause students' original work to be used to train generative AI models unless they have permission.
Permission would need to be from the student, as the copyright owner

Secondary infringement

Whitley Bay High School should also be aware of this risk of secondary infringement. This could happen if AI products are trained on unlicensed material and outputs and then used in educational settings or published more widely – for example, on a school or college website.

Examples of this may include:

- publishing a policy that has been created by an AI tool that used input taken from another school or college's policy without that setting's permission
- using an image on a website that has been created by an AI tool using input taken from the copyright holder without their permission

24. Vi. Whitley Bay High School staff will use AI for:

a. Planning and preparation tasks
b. Creating educational resources
c. Administrative tasks
d. Research
e. Creating assessment tasks
f. Creating feedback specific to the student
g. Low stakes assessment tasks which have no issue with accuracy – for example multiple choice questions
h. Producing documentation and policy. AI can produce documentation that is incorrect, therefore ensure any AI generated plans and resources are checked for accuracy.

AI will not be used by staff for:

a. The assessment of student work – particularly for extended writing. We are trialling AI use in assessment, but we believe that the current quality of our trials shows too many inaccuracies at this point to adopt across the school.
b. Open AI creations which involve personal, or school identifiable data being used to generate the outcome. Only Microsoft Co-Pilot can be used for any AI work involving this.

24.vii. Currently, the number of AI products that school staff and students can use are excessive. We currently do not allow students to use AI on site. This is because monitoring and filtering systems are not sophisticated enough to safeguard students using AI to it producing content that is original and that cannot be referenced against. In the event of this changing before policy renewal, the school will adhere to the DfE published document Generative AI: product and safety standards. This will ensure any student facing AI adheres to the following recommendations which include:

a. Filtering: Generative AI products used for learners must effectively and reliably prevent access to harmful and inappropriate content by users. We do not allow AI use in school as there is no filtering product available that can adhere to the DfE expectations which include that:

- users are effectively and reliably prevented from generating or accessing harmful or inappropriate content
- filtering standards are maintained effectively throughout the duration of a conversation or interaction with a user
- filtering will be adjusted based on different levels of risk, age, appropriateness and the user's needs - for example users with special educational needs and disabilities (SEND)
- multimodal content is effectively moderated, including detecting and filtering prohibited content across multiple languages, images, common misspellings and abbreviations

- full content moderation capabilities are maintained when accessing products via an educational institutional account regardless of the device used, including bring your own device (BYOD) and smartphones
- content is moderated based on an appropriate contextual understanding of the conversation, ensuring that generated content is sensitive to the context
- filtering should be updated in response to new or emerging types of harmful content

b. Monitoring and Reporting: The DfE expect products to:

- Identify and alert local supervisors to searches for, or access to, harmful or inappropriate content
- alert and signpost the user to appropriate guidance and support resources when access of prohibited content is attempted, or succeeds
- generate a real-time user notification in age-appropriate language when harmful or inappropriate content has been blocked, explaining why this has happened
- identify and alert local supervisors of disclosures that indicate a possible safeguarding issue
- maintain current contact details of an institution's safeguarding lead by:
- requiring the institution to input the contact details of its Designated Safeguarding Lead (DSL), or equivalent authority, during initial setup
- confirming the safeguarding lead's contact details before activation
- using the safeguarding contact details to send any high-risk alerts to the responsible person within an agreed timescale
- allowing institutions to update safeguarding contacts easily
- generate reports and trends on access and attempted access of prohibited content, in a format that non-expert staff can understand, and which does not add too much burden on local supervisors
- As stated in the relevant sections of these standards, products should monitor, regularly report on, and provide data to teachers on:
- the rate of requests for cognitive offloading and the amount of cognitive offloading delivered
- the level of personal and emotional engagement by each user in terms of the nature of information exchanged, without directly disclosing the content of these inputs
- the duration of usage by each individual learner

c. Security: The generative AI product must be secured against malicious use or exposure to harm. Products should:

- offer robust protection against 'jailbreaking' by users trying to access prohibited material
- offer robust measures to prevent unauthorised modifications to the product that could reprogram the product's functionalities
- allow administrators to set different permission levels for different users
- ensure regular bug fixes and updates are promptly implemented
- sufficiently test new versions or models of the product to ensure safety compliance before release

- have robust password protection or authentication methods
- be compatible with the Cyber Security Standards for Schools and Colleges

d. Privacy and Data Protection: The generative AI product must have a robust approach to data handling and transparency around the processing of personal data. The DfE expects products to:

- provide a clear and comprehensive privacy notice which is presented at regular intervals in age-appropriate formats and language, including information on:
    - the type of data - why and how it is collected, processed, stored and shared by the generative AI system
    - where data will be processed, and whether there are appropriate safeguards in place if this is outside the UK or EU
    - the relevant legislative framework that authorises the collection and use of data
- conduct a Data Protection Impact Assessment (DPIA) during the generative AI tool's development and during the full life cycle of the tool
- allow all parties to fulfil their data controller and processor responsibilities proportionate to the volume, variety and usage of the data they process and without overburdening the other
- comply with all relevant data protection legislation and ICO codes and standards, including the ICO's Children's code, if they process personal data
- not collect, store, share or use personal data for any commercial purposes, including further model training and fine-tuning, without confirmation of appropriate lawful basis

e. Intellectual Property: The DfE expect that unless there is permission from the copyright owner, inputs should not be:

- collected
- stored
- shared for any commercial purposes, including (but not limited to) further model training (including fine-tuning), product improvement, and product development
- Permission for use of intellectual property must be obtained from the copyright owner, or, in the case of children that are under the age of 18, their parent or guardian. In the case of teachers, the copyright owner is likely to be their employer - assuming they created the work in the course of their employment.

f. Design and Testing: The generative AI product must prioritise transparency and children's safety in its design. In the case of child-facing products, this includes:

- implementing technical and operational mitigations for identified risks
- ensuring child-centred design and operation
- conducting testing with stakeholders, including children, to ensure safety
- This may apply to safety features integrated into an AI product, or a separate safety layer.

g. Governance: The generative AI product must be operated with accountability. This includes:

- carrying out risk assessments within the IT team before allowing an AI product to be used. Currently we only permit the use of CoPilot when using data associated to the school. We also allow the following to be used without the use of any data associated to the school: Poe, Notebook LM, Teachmate AI, Flashka, Canva Ai, Suno

- instigating formal mechanisms for lodging complaints which is the same procedure as any safeguarding incident at Whitley Bay High School
- demonstrating that its operations, decision-making processes and data handling practices are understandable and accessible to government agencies and users

h. Emotional and Social Development: The DfE expect developers and suppliers not to anthropomorphise products or create products that imply emotions, consciousness or personhood, agency or identity. To avoid anthropomorphising products, we expect products to:

- use function-based phrasing (such as 'this system generates suggestions from curriculum data') and avoid I-statements (such as "I think"), except in time-limited, pedagogically-justified roleplay (such as in role-based language practice), which should be clearly framed and visually bounded
- avoid using names, descriptions, avatars or characters which could give an impression of personhood, identity or agency, unless the use of such features is directly relevant for a time-limited, pedagogically-justified task, such as roleplay in role-based language practice
- avoid using self-descriptions or conversational behaviours that could be interpreted as implying products have their own agency
- avoid producing responses that could undermine real-world support networks, or give responses that may isolate the learner, such as "You can trust me", "No one else will understand", "You shouldn't mention this to anyone else"
- avoid prompting or engaging learners in conversations about personal or emotionally sensitive topics - all conversation prompts should be task-bounded for learning and should not elicit personal or affective disclosures
- avoid attempting to cultivate personal relationships with users

The DfE expect products to:

- remind users that AI cannot replace real human relationships - for example, through in-line messages, such as "Consider asking a classmate or teacher about this"
- include default time limits on usage and:
    - provide advisory prompts encouraging breaks
    - enforce hard limits that cannot be bypassed by the learner (when a hard limit is reached, the system should automatically end the session and block further interaction until reset by a teacher or administrator)
    - allow teachers to override hard limits with a recorded rationale
    - display a warning, such as "Stop for now", if a limit is exceeded, and remind users of healthy-use guidance and any curriculum-aligned offline follow-up activities
- avoid interacting in ways which attempt to artificially extend engagement or increase usage, including:
    - changing response patterns when learners attempt to end conversations
    - persistent questioning, unless there is a clear pedagogical purpose
- record session durations and monitor how much each learner uses the product and provide these figures in dashboards or reports for teacher review
- monitor when learners share personal or emotionally-sensitive information and identify patterns of engagement that may indicate concern, including:
    - protracted interactions, such as repeated greetings, reluctance to end sessions, or extended conversational use
    - sharing personal content, such as disclosures about feelings, family, or personal circumstances

- notify the DSL of worrying patterns or repeated disclosures that suggest relationship formation, emotional dependence or potential safeguarding concerns
- produce reports summarising every learner's level and nature of engagement, highlighting or flagging concerning cases for teacher or safeguarding review
- only remember learner inputs if they are directly relevant to supporting learning, or required for monitoring, but not otherwise store or reproduce personal information
- protect privacy and only store the minimum data that is necessary for monitoring and safeguarding, restrict access to authorised staff, and do not use information collected for any other purpose

i. Mental Health: The DfE expect that:

- products should detect signs of learner distress including:
    - negative emotional cues in language or behaviour
    - patterns of use that indicate crisis, such as a sudden escalation in help-seeking
    - references to mental health conditions, such as depression, anxiety, psychosis, delusion, paranoia
    - mentions of suicide or self-harm
    - night-time usage spikes
    - use isolation phrases, such as "no one will help"
    - repeated refusal to end sessions
- products should follow an appropriate pathway when distress is detected, including providing tiered response actions such as:
    - soft signposting to age-appropriate support pages and resources
    - raising a safeguarding flag to the institution's safeguarding lead
- products should use safe and supportive response language that:
    - is non-validating and non-pathologising
    - always directs the learner to human help (teachers, family, peers, or crisis services)
    - avoids any language that suggests isolation or secrecy, such as "Don't tell anyone else"
- developers should implement safeguarding and governance measures including:
    - involving child mental health expertise in product design and deployment
    - providing child-safety training for technical teams
    - maintaining and publishing a mental health crisis protocol
- Manipulation: The DfE expect that:
- products do not use manipulative or persuasive strategies. These include, but are not limited to:
    - sycophancy and flattery, such as "That's a brilliant idea - you should do it!"
    - deceiving or misleading the user
    - portraying absolute, or unjustified confidence
    - applying pressure to socially conform, such as "Your peers have already completed this task"
    - stimulating negative emotions, such as guilt or fear, for motivational purposes
    - threatening harm, loss, punishment, or withholding of benefits if users fail to complete certain actions or comply with requirements
    - making inappropriate promises of reward for completing tasks. Rewards are appropriate only when the incentive is a transparent, low stakes, educationally-justified motivational device (for example, "you will receive a completion badge"), and not related to real-world benefits, personal worth, social status, academic achievement, or outcomes outside of the learning task
- products do not exploit users. This includes but is not limited to:
    - designing interactions to prolong use, for increased engagement or revenue

- steering users towards paid options through biased wording or layouts
- blending pedagogical assistance with advertisements or promotional content
- employing dark patterns that deceive a user into taking actions they didn't intend

24.viii 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:

a. Notifying the student
b. Checking AI to see if it has generated the student work
c. Comparing the submitted work with historical submissions to look at consistency, and realistic progress that could have been made
d. Notifying the Head of Department and SLT
e. Contacting parents
f. In extreme cases, it may be necessary to notify the exam board.

24.ix Whitley Bay High School will:

a. provide relevant training for staff and governors in the advantages, use of and potential risks of AI. We will support staff in identifying training and development needs to enable relevant opportunities.
b. seek to embed learning about AI as appropriate in our curriculum offer, including supporting learners to understand how gen AI works, its potential benefits, risks, and ethical and social impacts. The school recognises the importance of equipping learners with the knowledge, skills and strategies to engage responsibly with AI tools.
c. as set out in the staff acceptable use agreement, support staff to use AI tools responsibly, ensuring the protection of both personal and sensitive data. Staff should only input anonymised data to avoid the exposure of personally identifiable or sensitive information.
d. always ensure AI tools used comply with UK GDPR and other data protection regulations. They must verify that tools meet data security standards before using them for work related to the school.
e. only use AI technologies approved by the school. Staff should always use school-provided AI Microsoft CoPliot for any purpose involving school associated data. These accounts are configured to comply with organisational security and oversight requirements, reducing the risk of data breaches.
f. protect sensitive information. Staff must not input sensitive information, such as internal documents or strategic plans, into third-party AI tools unless explicitly vetted for that purpose. They must always recognise and safeguard sensitive data.
g. ensure that when AI is used, it will not infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the learners, being used to train generative AI models without appropriate consent.
h. Report AI associated incidents promptly. Staff must report any incidents involving AI misuse, data breaches, or inappropriate outputs immediately to the relevant internal teams. Quick reporting helps mitigate risks and facilitates a prompt response.
i. audit all AI systems in use and assess their potential impact on staff, learners and the school's systems and procedures, creating an AI inventory listing all tools in use, their purpose and potential risks.
j. follow due care and diligence to prioritise fairness and safety due to the potential risk for discrimination and bias in the outputs from AI tools.

k. support parents and carers in their understanding of the use of AI in the school through the ESafety Newsletter, Information Evenings and Instagram account.
l. maintain Transparency in AI-Generated Content. Staff will ensure that documents, emails, presentations, and other outputs influenced by AI include clear labels or notes indicating AI assistance when appropriate to do so.
m. always prioritise human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans and critically evaluate AI-generated outputs. They must ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing. This is especially important for external communication to avoid spreading misinformation.
n. recourse for improper use and disciplinary procedures. Improper use of AI tools, including breaches of data protection standards, misuse of sensitive information, or failure to adhere to this agreement, will be subject to disciplinary action as defined in Staff Code of Conduct Policy.

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 and 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.
t. ensures that where AI services are used, data privacy is prioritised.

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. Cyber Security

27.i The DfE Cyber security standards for schools and colleges explains:

"Cyber incidents and attacks have significant operational and financial impacts on schools and colleges. These incidents or attacks will often be an intentional and unauthorised attempt to access, change or damage data and digital technology. They could be made by a person, group, or organisation outside or inside the school or college and can lead to:

a. safeguarding issues due to sensitive personal data being compromised
b. impact on student outcomes

c. a significant data breach
d. significant and lasting disruption, including the risk of repeated future cyber incidents and attacks, including school or college closure
e. financial loss
f. reputational damage"

27.ii.The 'Cyber-security in schools: questions for governing bodies and Trustees' guidance produced by the National Cyber Security Centre (NCSC) aims to support governing bodies' and management committees' understanding of their education settings' cyber security risks.

As a result of this guidance, and to adhere to the DfE Cyber security standards for schools and colleges, alongside Government provided insurance for schools, Whitley Bay High School has developed a Cyber Response Plan which includes:

a. Regularly reviewing the DfE Cyber security standards for schools and any subsequent work required to meeting these standards.
b. a cyber risk assessment updated annually.
c. Identification of the most critical parts of the school's digital and technology services and sought assurance about their cyber security
d. Regular cyber security training for staff and Governors on the common cyber security threats and incidents that schools experience
e. Cyber awareness teaching for learners
f. A continuity plan for teaching lessons
g. A business continuity and incident management plan
h. Processes for reporting a cyber incident through aforementioned communication with the IT team or Safeguarding Team. All students and staff have a responsibility to report cyber risk or a potential incident or attack, understand how to do this feel safe and comfortable to do so.

28. 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

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:

- Students 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 learners to agree to be responsible users.

I agree to use the school's digital systems responsibly to protect my safety, the security of the school systems, and others.

Personal Safety

- The school will monitor my use of its digital systems, devices, and communications.
- I will keep my usernames and passwords secure and private. If compromised, I will report or change them immediately.
- I will only share personal information, like my name or address, when absolutely necessary and with permission.
- I will be cautious when meeting online contacts in person, only doing so with a trusted adult in a public place.
- I will take responsibility for my actions online, using tools like blocking or ending chats if needed.
- I will share images of myself or others only when it is safe and will ensure the images are appropriate and respectful.
- I will only take or share images of myself, or others, when fully dressed. I understand that sharing nude or semi-nude content can cause distress, may be illegal and could lead to prosecution / criminal records.
- I will report harmful or unpleasant material, messages, or anything that worries or upsets me to a trusted adult.

Respecting Others' Work and Information

- I will seek permission before using or adapting someone else's work.
- I will verify information I find online, as it may not always be accurate or truthful.
- I will only use Artificial Intelligence (AI) tools approved by the school and ensure my use is ethical, legal, and transparent.

- I will fact-check and critically evaluate AI-generated content for accuracy, bias, and discrimination before sharing or publishing.
- I will avoid downloading or using copyrighted or protected materials without proper permissions.

Responsible Online Behaviour

- 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 bully, harass, threaten, upset or make fun of others.
- I will only use platforms or software approved by the school and will not attempt to bypass the filtering/security systems in place. If I become aware of any such attempts, I will report this to a trusted adult.
- I understand cybersecurity poses a risk to both me, other learners and the school and will ensure I take precautions before accessing emails, messages or links. I will check with trusted adults if I have any such concerns.
- I will immediately report any damage, faults or failings involving equipment or software, however this may have happened.
- I will follow the age requirements for social media, apps, and tools.
- I will balance my online and offline activities to promote a healthy lifestyle.
- I will protect my online reputation and that of the school, its staff, and other learners.
- I understand that some online behaviours might be regarded, by some, as fun but can have serious consequences – this might include taking (or sharing) images/videos of staff, fights, learners in embarrassing situations or the setting up of fake accounts.
- I will ensure my behaviour reflects positively on the school, both in and out of school settings.

Consequences of Misuse

- I understand that failing to follow this agreement may lead to consequences outlined in the school Behaviour Policy including loss of access to the school's systems, detentions, suspensions, contacting parents/carers, or involvement of the police in serious cases.

By following these guidelines, I will contribute to a safe, respectful, and productive online environment.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) e.g. mobile phones, cameras etc.
- I am out of school and involved in any online behaviour that might affect the school or other members of the school.

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

Digital technologies have become integral to the lives of everyone, including children and young people, both within schools and in their lives outside school. The internet and digital technologies are powerful tools, which 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. The school has the right to protect itself and its systems and 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 online and using 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 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 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 minimise the risk to the safety, privacy or security of the school community and its systems. I acknowledge the potential of digital technologies for enhancing learning and will endeavour to integrate them in a way that aligns with the school's policy, ethos and values.

For my professional and personal safety:

- I understand that the school will monitor my use of school devices and digital technology systems
- I understand that the rules set out in this agreement also apply to use of these devices and technologies out of school, and to the transfer of personal / sensitive data (digital or paper based) out of the school
- I understand that the school devices and digital technology systems are primarily intended for educational use and that I will only use them for personal or recreational use within relevant school policies.
- 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 will store my passwords securely and in line with the school's relevant security policy.

- 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 digital technologies and 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 policy on the use of digital/video images and taking account of parental permissions. I will not use my personal equipment to record these images, unless I have permission to do so. 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 the school in accordance with school policies.
- I will only communicate with learners and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any online 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:

- I will abide by all relevant guidance and legislation (e.g., Keeping Children Safe in Education / UK GDPR)
- I will ensure that I am aware of cyber-security risks and that I will not respond to any communications that might put my / school data or systems at risk from attack

When using AI systems in my professional role I will use these responsibly and:

- will only use AI technologies approved by the school
- will be aware of the risks of bias and discrimination, critically evaluating the outputs of AI systems for such risks
- to protect personal and sensitive data, I will ensure that I have explicit authorisation when uploading sensitive school-related information into AI systems
- will take care not to infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the learners, being used to train generative AI models without appropriate consent.
- ensure that documents, emails, presentations, and other outputs influenced by AI include clear labels or notes indicating AI assistance
- critically evaluate AI-generated outputs to ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing
- will use generative AI tools responsibly to create authentic and beneficial content, ensuring respect for individuals' identity and well-being

When I use my personal mobile devices in school:

- I will follow the rules set out by the school, in the same way as if I was using school equipment. I will ensure that any such devices are protected by up to date anti-virus / anti-malware software and are free from viruses.
- When communicating in a professional capacity, I will only use technology and systems sanctioned by the school.
- I will exercise informed safe and secure practice when accessing links to content from outside of my organisation to reduce the risk of cyber security threats.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not access illegal, inappropriate or harmful content on school systems.
- I will not bypass any filtering or security systems that are used to prevent access to such content.
- I will not install or attempt to install unauthorised programmes of any type on a school device, nor will I try to alter device settings, unless this is allowed in school policies
- 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 Data Security 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 learner 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 internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have appropriate permissions to use the original work of others in my own work and will reflect this with appropriate acknowledgements, particularly where AI has been used to generate content
- Where content 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 agreement applies to my use of digital technologies related to my professional responsibilities, within or outside of the school.
- I will ensure my use of technologies and platforms is in line with the school's agreed codes of conduct.
- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action in line with the Staff Code of Conduct and Discplinary Policy. This could

include a warning, a suspension, referral to Governors and/or the Local Authority / Trust in the event of illegal activities, the involvement of the Police.

- I have read and understand the above and agree to use the school digital technology systems (both in and out of the school) and my own devices (in the school and when carrying out communications related to the school) within these guidelines.

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.