Adopted by Full Governors 27.01.2022 Item 7c

Whitley Bay High School

E-Safety Policy

Update Proposed: September 2022

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

- ESafety documentation released by the Government and Local Authority in July 2020 regarding student laptops funded by the DfE for disadvantaged Year 10 students.
- Teaching Online Safety in School June 2019: https://www.gov.uk/government/publications/teaching-online-safety-in-schools
- 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
- SWGfl: https://swgfl.org.uk/resources/online-safety-policy-templates/
- Keeping Children Safe in Education 2021
- 360 Degrees Safe website: https://360safe.org.uk/about-the-tool
- UK Safer Online Centre Website: http://www.saferinternet.org.uk/
- Child Exploitation and Online Safety Website: http://ceop.police.uk
- The Education People: https://www.theeducationpeople.org/media/4472/online-safety-within-kcsie-2021.pdf
- Keeping Children Safe Online Government Publication: Coronavirus (COVID-19): support for parents and carers to keep children safe online - GOV.UK (www.gov.uk)
- Think u Know website (and App – from NCEA and CEOP) Thinkuknow - home

1. Development / Monitoring / Review of this Policy

1.1 This e-safety policy has been developed by the Curriculum and Student Affairs (CSA) Governing Body working group made up of:

- Headteacher
- Designated Safeguarding Lead (Deputy Headteacher)
- E-Safety Leader (Deputy Headteacher)
- Staff including Deputy Designated Safeguard Leads
- Governors of the CSA committee

2. Schedule for Development / Monitoring / Review

2i. This e-safety policy was approved by the Curriculum and Student Affairs Governing Body on:	
2ii. The implementation of this e-safety policy will be monitored by the:	E-Safety Deputy Headteacher / Network Manager / Curriculum and Student Affairs Committee and Senior Leadership Team.
2iii. Monitoring will take place at regular intervals:	September every year
2iv. The Governing Body will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	As part of Safeguarding updates in Full Governors when necessary
2v. The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	September every year
2vi. Should serious e-safety incidents take place, the following external persons / agencies should be informed:	Senior Leadership Team (SLT) – DSL (Designated Safeguarding Lead) / DpDSL (Deputy Designated Safeguarding Lead) Police Front Door LADO

2vii. The school will monitor the impact of the policy using:

- Logs of reported incidents on CPOMS
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys / questionnaires of
    - students
    - parents / carers
    - staff

3. Scope of the Policy

3i This policy applies to all members of the school community (including staff, governors, students, volunteers, parents / carers, visitors, community users) who have access to and are ***users of school digital technology systems***, both in and out of the school.

3ii The school will deal with such incidents within this policy along with associated behaviour and anti-bullying policies and will, where known, inform parents of incidents of unsuitable e-safety behaviour that take place out of school in line with

the Education and Inspections Act 2006 and 2011. The response to incidents of unsuitable e-safety behaviour that take place in school will be in line with the school's Behaviour Policy. If an incident is more appropriate for child protection, such as in the form of peer to peer abuse; intervention will be in line with the Child Protection Policy.

4. Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school:

4.1 Governors:

4.1i Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the full Governors and Curriculum and Student Affairs Governors Sub Committee receiving regular information about e-safety incidents and monitoring reports. Joan Bloomfield has taken on the role of E-Safety Governor as part of her Safeguarding Governor role. This role includes meeting the E-Safety Leader (Deputy Headteacher) and ICT team to:

- Monitor any e-safety safeguarding incidents
- Attend safeguarding training which includes e-safety
- Ensure e-safety and security systems are up to date
- Monitor and review logs of online safety controls including Securus and Smoothwall
- Provide reports and updates to the Full Governing Body when necessary

The Governing Body will receive any relevant e-safety update as part of the Safeguarding update in Full Governors.

4.2 Headteacher and Senior Leaders:

a. The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Deputy Headteacher.

b. The Headteacher, DSL and DpDSL are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see flow chart on dealing with e-safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority disciplinary procedures as part of our Child Protection Policy).

c. The Headteacher is responsible for ensuring that the E-Safety Deputy Headteacher, DSL and DpDSL receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

d. The E-Safety Deputy Headteacher 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 e-safety monitoring role as recommended by North Tyneside Safeguarding Board. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

e. The Senior Leadership Team will receive monitoring reports from the IT network team when requested.

f. The Headteacher ensures training records are held which accurately record e-safety and safeguarding CPD for staff.

4.3 E-Safety Deputy Headteacher:

4.3i As E-Safety lead, the Deputy Headteacher and DpDSL will:take day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies

a. ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place

b. provides training and advice for staff

c. liaise with the Local Authority and regular external agencies

d. liaise with school technical staff and the ICT department during weekly strategy meetings which reviews e-safety

e. receive reports of e-safety incidents and create a log of incidents to inform future e-safety developments – this log will be kept as part of the secure child protection logs using CPOMS.

f. meet with Safeguarding and E-Safety Governor to discuss current issues, review and change incident logs and filtering
g. attend relevant meetings to update Governors committees
h. report regularly to Senior Leadership Team
i. be responsible for ensuring that all e-safety education is updated regularly and communicated with students in conjunction with the Personal Development Coordinator through LEV, tutorials, assemblies and other relevant areas both in and out of the curriculum
j. Work with the Personal Development Co-ordinator to ensure e-safety is embedded in all aspects of the curriculum and other activities.

4.3ii 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 e-safety behaviour.

4.4 Network Manager and Technical staff:

4.4i The Network Manager and technical staff are responsible for ensuring:

a. that the school's technical infrastructure is secure and is not open to misuse or malicious attack
b. that the school meets required e-safety technical requirements and any North Tyneside Local Authority E-Safety Policy and guidance that may apply.
c. that users may only access the networks and devices through a properly enforced password protection and Acceptable Use Policy.
d. the recommended North Tyneside filtering policy (Smoothwall) is applied and updated on a regular basis alongside Securus monitoring software.
e. that the implementation of this software is not the sole responsibility of any single person but the ICT team.
f. the ICT team keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
g. that the use of the network / internet / SharePoint / OneDrive / remote access / email / ~~school~~ social media is monitored in order that any misuse / attempted misuse can be reported to the E-Safety Deputy Headteacher/ DSL/ DpDSL for investigation
h. that monitoring software systems are implemented and updated as agreed in school
i. The team access training through external courses and Governing Body expertise to ensure the e-safety strategy is frequently improved

4.5 Teaching and Support Staff

4.5i Teaching and Support Staff are responsible for ensuring that:

a. they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
b. they have read, understood and clicked that they agree the Staff Acceptable Use Policy (AUP) available in the staff handbook and when they log onto the network
c. they report any suspected misuse or problem to the Headteacher / E-Safety Deputy Headteacher / DSL / DpDSL for investigation
d. all digital communications with students / 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.
e. e-safety issues are embedded in all aspects of the Personal Development and subject curriculums (where relevant) as well as extracurricular activities
f. students understand and follow the e-safety and Acceptable Use Policy
g. students have a good understanding of research skills and the need to avoid plagiarism
h. when permission is given to students, they monitor the appropriate use of digital technologies, mobile devices, cameras etc in lessons, and other school activities (where allowed) and implement the recommendations of the E-Safety Policy whilst using these devices
i. in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

4.6 DSL / DpDSL (Currently 14 staff in school)

4.6i The DSL and DpDSL should be trained in e-safety and be aware of the potential for serious child protection / safeguarding issues to arise from:

a. sharing of personal data
b. access to illegal / unsuitable materials
c. unsuitable on-line contact with adults / strangers
d. potential or actual incidents of grooming
e. cyber or online bullying
f. Prevent Strategy and Radicalisation
g. Sexting
h. Accessing and hacking into secure networks
i. County lines and use of the local Metro system
j. Cyber crime
k. abusive, harassing, and misogynistic messages,
l. 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 Child Protection Policy and will be actioned as in line with the recommendations of these documents.

4.7 Students:

a. are responsible for using the school ICT systems and their own devices in accordance with the Pupil Acceptable Use Policy
b. have a good understanding of research skills and the need to avoid plagiarism
c. need to understand the importance of reporting abuse, misuse or access to unsuitable materials and know how to do so. This includes both face to face and online abuse.
d. will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber/online bullying.
e. should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy could cover their actions out of school if it relates to their membership of the school. The school cannot be held responsible for student actions regarding internet use and social media outside of school hours.
f. should alert their teacher if they have not provided consent to activities which may leave an ICT footprint and be in breach of their GDPR. Examples could include a photograph being used on the school website.
g. should act responsibly when loaning a school digital device which could include an Ipad, laptop or Chromebook.
h. Must adhere to the Student Acceptable Use Policy, when online and using their mobile or own device through a personal network such as 4G or 5G.

4.8 Parents / Carers

4.8i Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, the Home School Agreement, the website (Safeguarding and ESafety Section), School Twitter and via letters home. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

a. digital and video images taken at school events
b. access to parents' sections of the website / Sharepoint / OneDrive and on-line student records
c. their children's personal devices in the school (where this is allowed)
d. their children's use of technology, including social media in and out of school
e. their children's understanding of data protection and privacy

4.8ii In the event of an e-safety incident, both on a student owned or school device which could include cyber bullying, homophobia, racism or sexting outside of school, parents will be informed and usually advised to report the illegal or discriminatory act to the Police.

4.9 Community Users

4.9i Community Users who access school systems / website / Office 365 as part of the wider school provision will be expected to sign a Community User AUP (Acceptable Use Policy) before being provided with access to school systems. This will be digitally signed for at the front office on arrival to the school. Community users, if permission is provided, will only be able to access the school Guest network.

5 Policy Statements

5.1 Education – students

5.1i Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience. The breadth of issues classified within e-safety is considerable, but is categorised into four areas of risk in the Keeping Children Safe in Education 2021 document. They are:

- 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: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.
- Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Deputy Headteacher in charge of e-safety.

Our e-safety and Personal Development curriculum has been planned using the key documents identified on the front page of this policy, with age appropriate content delivered across all key stages.

5.1ii E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

a. A planned e-safety curriculum which incorporates the four Cs above, should be provided as part of Personal Development, LEV and other lessons and should be regularly revisited
b. Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial activities
c. Students should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information.
d. Students should be taught to acknowledge appropriate and relevant academic sources of information when accessing resources on the internet
e. 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
f. Students should be supported to build resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision making. The school will continue to use monitoring and filtering software to ensure pupils are safe from terror and extremist material online
g. Staff should act as good role models in their use of digital technologies the internet and mobile devices
h. in lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
i. Staff should be vigilant in monitoring the content of websites the young people visit during lessons.
j. It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need and reviewed by the ICT network team during the weekly meeting.
k. Students need to be aware of the potential for online sexual harassment. This may be standalone, or part of a wider pattern of sexual harassment and/or sexual violence. It may include:

i. consensual and non-consensual sharing of nudes and semi-nudes images and/or videos.
ii. taking and sharing nude photographs of U18s which is a criminal offence
iii. sharing of unwanted explicit content
iv. upskirting (which is a criminal offence)
v. sexualised online bullying
vi. unwanted sexual comments and messages, including, on social media
vii. sexual exploitation; coercion and threats

5.1iii As part of students Personal Development Curriculum in school, LEV, assemblies and pastoral tutor groups will all be educated on the underpinning knowledge and behaviors which keep students safe from harm as suggested by the DfE Teaching Online Safety in Schools 2019 document and within Keeping Children Safe in Education 2021 document. This includes:

a. How students evaluate what they see online
b. How students recognize techniques used for persuasion
c. How to recognise acceptable and unacceptable online behavior
d. How to identify online risks
e. How to seek support

5.2 Education – parents / carers

5.2i Many parents have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and unsuitable material on the internet and may be unsure about how to respond.

5.2ii The school will therefore seek to provide access to this policy and other guidance through curriculum activities, the website (Safeguarding and ESafety section), school Twitter high profile events (e.g. Safer Internet Day) and information evenings.

5.2iii Parents are encouraged to support the school and their children to adhere to the Student Acceptable Usage policy whilst using the school's and their own network whilst on school site.

6 Education & Training

6.1 Staff / Volunteers

6.1i It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered via:

a. A planned programme of formal e-safety training which will be made available to staff as part of the annual Safeguarding update. This will be regularly updated and reinforced by the DSL, DpDSL and Network Manager at least annually.
b. All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policy
c. The E-Safety Deputy Headteacher or Network Manager will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
d. This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days. This will usually be conducted through safeguarding training and pastoral Year Team training.
e. The E--Safety Deputy Headteacher or Network Manager will provide advice / guidance / training to individuals as required.

6.2 Training – Governors

6.2i Governors should take part in e-safety training. This can be as part of the annual update to safeguarding children, but also via the Local Authority, National Governors Association or any other relevant organisation.

6.2ii Governors are welcomed to attend Governance training in e-safety through external courses in order to support and challenge the school on e-safety procedures.

7 Technical – infrastructure

7.1 Equipment, filtering and monitoring

7.1i The school will be responsible for ensuring that the school infrastructure and network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

a. School technical systems will be managed in real time in ways that ensure that the school meets recommended technical requirements outlined by North Tyneside LA
b. There will be regular reviews and audits of the safety and security of school technical systems using external support and Governance expertise.
c. Servers, wireless systems and cabling must be securely located and physical access restricted
d. All users will have clearly defined access rights to school technical systems and devices.
e. All users will be provided with a username and secure password by the Network Manager (or ICT team member) who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password. Students will be regularly reminded to press windows and L to lock their screen.
f. The Network Manager must ensure passwords are secure but available to the headteacher, DSL or DpDSL if required.
g. The Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
h. Internet access is filtered for all users as recommended by North Tyneside LEA. The filtering system protects students without causing a negative impact on their education. Illegal content is filtered by the Local Authority broadband filtering provider by actively employing the internet Watch Foundation CAIC lists. Content lists are regularly updated and internet use is logged and regularly monitored. Any filtering changes requested by staff must be approved by the E-Safety Deputy Headteacher in conjunction with the DSL.
i. Internet filtering via Smoothwall and monitoring via Securus will ensure that students are safe from terrorist and extremist material whilst accessing the internet.
j. School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Policy. This is discussed and recorded in the weekly network meeting.
k. Users report any actual / potential technical incident / security breach to the ICT team and potentially the Headteacher, DSL or DpDSL.
l. Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from viruses, 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 virus software.
m. An agreed policy is in place for the provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the school systems. This involves the Acceptable Use Policy for all staff as outlined in Section E of the Staff Handbook.
n. An agreed Acceptable Use Policy is in place regarding the extent of personal use that users (staff / students / community users) and advises that school devices should not be used by others. This is outlined in Section E of the staff handbook.
o. An agreed Acceptable Use Policy is in place that forbids staff from downloading executable files and installing programmes on school devices.
p. An Acceptable Use Policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. USB ports have been disabled within school and personal data should only be sent online or stored locally if encrypted and password protected. This is in line with the school’s GDPR policy.

7.2 Mobile Technologies (including Bring Your Own Device (BYOD))

7.2i Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, 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’s Office 365, Sharepoint and Onedrive and other cloud based services such as email and data storage. All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational.

7.2ii Mobile technologies used in school will have access to Wi-fi with all users agreeing to the Acceptable Usage Policy. Whilst on this network, any users will be subject to the same secure access, filtering, data protection, storage and transfer

of data, mobile device management systems, training, support, acceptable use, auditing and monitoring as any other system in the school.

7.2iii The E-safety policy BYOD section incorporates and aligns to other active school policies which include Child Protection, Behavior Policy, Staff Handbook Section E and Acceptable Usage Policies (available in the appendicies).

7.2iv The table below summarises how the school will used mobile technologies on school owned, student, staff and visitor devices.

	School Mobile Devices	Student Personal Mobile Device	Staff Owned Personal Mobile Device	Visitor Owned Personal Mobile Device
Allowed in school	Yes	Yes	Yes	Yes
Full network access	Yes	No	No	No
Guest wi-fi network access Only	No	Yes	Yes	Yes
Monitoring and filtering of devices whilst on Guest Network	Yes	Yes	Yes	Yes
Technical Support in school	Yes	Support available when using school wi-fi	Yes	Yes
Access to school Sharepoint and Onedrive	Yes	Yes	Yes	No
Access to school personal and shared drives	No	No	No	No
App Installation	Yes	No	No	No
Sensitive Data Storage (see below for data protection and images including video)	No	No	No	No
Is the school liable for damage?	Yes	No	No	No
Access to a personal network	No	Yes	Yes	Yes
Does the Staff and Student Acceptable Use Policy apply on site whilst using own network?	Yes	Yes	Yes	Yes

7.2v. The school will do its best to enable students and staff to use their own devices as outlined above. The school however does not take any responsibility for maintenance, accidental damage, misuse, loss or theft of property. Students and staff who are particularly concerned about this, are advised to check their own home insurance for coverage.

7.2vi The school permits use of a students device in order to support learning, organisation and in preparation for work. We do acknowledge 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, could access social media, become involved in peer on peer abuse or sexually harass their peers via their mobile and smart technology. This includes sharing indecent images: consensually and nonconsensually (often via large chat groups), and view and share pornography and other harmful content as outlined in the Keeping Children Safe in Education 2021 publication. Consequently, students who use their own devices are expected to apply the same Acceptable Use Policy to their device whilst connected to their personal network in school.

8 Use of digital and video images

8i. 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. As part of the school GDPR, some students have also opted to consent for their image being used online. Students are expected to inform staff if their image is being taken and they haven't provided consent. Staff, parents and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying 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. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

a. When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet, on social networking sites.

b. In accordance with GDPR guidance, all students will have to provide consent for their image to be used online or in school publications.

c. In accordance with guidance from the Information Commissioner's Office, parents 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 comment on any activities involving other students in the digital / video images.

d. Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Students may request that they are not on anything that is published on line or in school as part of their GDPR consent. Digital images on staff devices should be transferred as soon as possible from their phones/tablets/personal computers to the staff storage areas before being removed.

e. Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

f. Students must not take, use, share, publish or distribute images of others without their permission

g. Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.

h. The GDPR consent agreement allows students to opt out of their photograph and work being published on the school website or Twitter account.

i. Student full names will only be used on school online platforms if consent has been given in line with GDPR.

j. Student work can only be published with the permission of students in line with GDPR.

k. Students will be educated on the risks of sexting, upskirting and sharing nude and semi-nude images online through the Personal Development curriculum.

In the event of a member of staff dealing with a sensitive incident involving anything in point K, we will follow the Child Protection Policy and ensure no member of staff views an illegal photo or forward it on.

9 Data Protection

The school is responsible for ensuring an appropriate level of digital security protection in place. As cyber crime continually evolves, the school will access training and advice from areas of expertise within the Governing Body, but also through external providers to provide a safe and secure IT system.

9i With effect from 25th May 2018, the data protection arrangements for the UK change following the European Union General Data Protection Regulation (GDPR) announced in 2016. Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

9ii. Please refer to our GDPR section (https://www.whitleybayhighschool.org/lower-school/gdpr) on the website and the school Data Protection Policy for further information.

9iii. In line with GDPR, the school will ensure that:

a. It has paid the appropriate fee to the Information Commissioner's Office (ICO).

b. It has appointed a Data Protection Officer (DPO).

c. It has a Data Protection Policy

d. it has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest.

e. it has an 'information asset register' in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it

f. the information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded
g. it will hold only the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for. The school should develop and implement a 'retention policy" to ensure there are clear and understood policies and routines for the deletion and disposal of data to support this. personal data held must be accurate and up to date where this is necessary for the purpose it is processed for. Have systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
h. it 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 (https://www.whitleybayhighschool.org/lower-school/gdpr)
i. we follow the school Subject Access Request procedures to deal with the individual rights of the data subject (subject to certain exceptions which may apply).
j. data Protection Impact Assessments (DPIA) are carried out if necessary.
k. IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring fenced from systems accessible in the classroom/to learners
l. it has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.
m. it understands how to share data lawfully and safely with other relevant data controllers.
n. it reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach in accordance with UK data protection 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.
o. We follow our Freedom of Information Policy which sets out how it will deal with FOI requests (due to be ratified by Governors).
p. all staff receive data protection training 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.

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

- data must be encrypted and password protected.
- device must be password protected. (be sure to select devices that can be protected in this way)
- device must be protected by up to date virus and malware checking software
- data must be securely deleted from the device as soon as possible.

9iv. 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 understands their rights and know how to handle a request whether verbal or written. Know who to pass it to in the school
d. where personal data is stored or transferred on mobile or other devices (including USBs) these must be encrypted and password protected.
e. will not transfer any school/academy personal data to personal devices
f. access personal data sources and records 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

9v. The school has disabled all USB ports from September 2018 to ensure school IT systems minimise the risk of a data breach resulting from hardware use.

10 Communications and Remote Learning

10i. A wide range of rapidly developing communications technologies has the potential to enhance learning. Mobile devices can be used during lessons to enhance learning, but only in conjunction with staff permission and the Child Protection, Esafety and Behaviour policy. In the result of a lockdown, staff will also be able to use Office applications as part of remote learning.

10ii. When using communication technologies the school considers the following as good practice:

a. The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).

b. Users must immediately report, to a DSL or DpDSL – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
c. Remote learning which could include videoed lessons, live lessons, theoretical information and lesson tasks should only be delivered through the Office 365 suite (Teams, Outlook etc)
d. Live lessons, although part of the school's remote learning strategy, should only be delivered and shared through the use of Microsoft Teams or Microsoft Stream. A small selection of staff who are part of the Student Welfare team have permission from the Headteacher to use more suitable applications or programmes.
e. Staff must be appropriately dressed and in a suitable location if conducting a remote lesson in the form of a 'video' or 'live lesson' from home. Staff should spend as little time as possible with their face in the background, aiming to share their screen as soon as they can.
f. Students should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with unsuitable communications and be reminded of the need to communicate appropriately when using digital technologies. This is largely part of the pastoral education of students and relates directly to the document Teaching Online Safety in Schools 2019.
g. Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.
h. Any digital communication between staff and students or parents and carers must be professional in tone and content.

11 Social Media

11i. Social Media is defined as

"Web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system."

Common examples of social media include facebook, Instagram, Twitter and Snapchat.

11ii. This section should also be read in conjunction with the following school documentation:

- Equality Policy
- Section E of the Staff Handbook
- Safeguarding and Child Protection Policy Guidance
- Disciplinary Policy and Procedures
- Guidance on Cyberbullying
- Keeping Children Safe in Education 2021 Statutory Guidance
- Guidance relating to the School E-Learning Strategy
- Teacher Standards issued by the DfE
- Teaching Online Safety in School June 2019
- DfE Relationships Education, Relationships and Sex Education (RSE) and Health Education 2019 Guidance

11iii. All schools, academies and local authorities have a duty of care to provide a safe learning environment for students and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

11iv. The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students, staff and the school through limiting access to personal information:

a. Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
b. Clear reporting guidance, including responsibilities, procedures and sanctions
c. Risk assessment, including legal risk
d. Ensuring personal information is not published unless consent is provided.

11v. School staff should ensure in their own personal social media that:

a. No reference should be made in social media to students, parents or school staff
b. They do not engage in online discussion on personal matters relating to members of the school community

c. Personal opinions should not be attributed to the school or local authority
d. Security settings on personal social media profiles are the responsibility of staff who we advise to regularly keep up to date.
e. They do not assign any pupil as a 'friend'/contact on their social media page, or any former pupil under the age of 18 or within the current academic year is prohibited, and caution should be taken regarding becoming assigned as a 'friend' with children of school age on the roll of another school or ex-students especially where siblings continue to attend the school. In addition, workers should never use, access, or become assigned as a "friend" of the social media pages of pupils on the roll of the school, or former pupils under the age of 18[1]. If in doubt please seek advice from your Headteacher/Deputy Head in charge of E-Safety.
f. The email address used to create the account is personal to them and not the whitleybayhighschool.org business address
g. When commenting, uploading or posting links within social media sites, remarks must never be derogatory, offensive, reflect negatively on your professionalism or that of colleagues or have the potential to bring the school into disrepute. Where workers become aware of such remarks made by others on social media platforms they should refer these immediately to the Headteacher.
h. They review the social media sites they participate in when joining the school, ensuring information available publicly about them is accurate and not inappropriate (e.g. photographs that may cause embarrassment to themselves and the school if they are published outside of the site).
i. They do not release any confidential information about themselves, the school, its employees, pupils, partners, or other stakeholders within the community.
j. They communicate to the Headteacher or DpDSL Esafety lead any occasions when there are social contacts between pupils and workers. For example where the parent and teacher are part of the same social circle. However, these contacts will be easily recognised and should be made known to the Headteacher where there may be implications for the adult and their position within the school setting.
k. any unsuitable material of a safeguarding nature uncovered relating to workers' activities both on public and private spaces within a social media site is reported to the Headteacher, who will determine the appropriate action inclusive of reporting to external agencies.
l. They are aware of the effect their actions may have on their image, actions that may cause offence intended or otherwise, as well as that of the school. Information that workers publish/post may be in the public domain for many years.
m. They are aware that the Governing Body will not accept any form of bullying or harassment of or by workers engaged by the school, inclusive of that through social media, commonly referred to as "cyber bullying". This may:

    - maliciously spreading rumours, lies or gossip
    - intimidating or aggressive behaviour
    - offensive or threatening comments or content
    - posting comments/photos designed to cause offence e.g. deliberately mocking an individual with the intent to harass or humiliate them

11vi. School social media accounts must be approved by the DpDSL in charge of e-safety. These accounts are only acceptable on Twitter (except one Instagram site for School Direct) and are monitored via Tweetdeck and staff must be prepared to declare usernames and passwords. The school's use of social media is to share and advertise what we do, not to engage in communications with followers. Any direct communication regarding complaints, will be replied to with a generic invitation to contact the school.

11vii. Serious breaches and misuse of social media by school employees could amount to gross misconduct and may result in dismissal. The below list constitutes examples of serious breaches but this list is not exhaustive:

- Breach of confidentiality/copyright
- Behaving in a discriminatory, bullying or harassing way towards others.
- Bringing the school or a partner agency into disrepute
- cyberbullying
- Where a criminal offence has taken place
- Unsuitable material that is of a safeguarding nature

11viii. Any worker who feels that a serious social media breach has occurred should inform the headteacher/Deputy Head in charge of E-Safety

11ix Monitoring of Public Social Media:

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school will respond to social media comments with a generic invitation to contact the school to discuss with a relevant member of staff. Social media can be used as a tool to vent, and the school has no wish to resolve personal issues in a public forum.

The *school's* use of social media for professional purposes will be checked regularly by the IT team to ensure compliance with the school policies.

12 Unsuitable Activities

12i. The school believes that the activities referred to in the following section would be unsuitable in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978. This includes self generated images typically referred to as sexting, or images obtained from upskirting, sexual harassment, or sexual violence.					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	Cyberbullying (including peer on peer abuse) and any threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Activities that might be classed as cyber-crime under the Computer Misuse Act: • 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						X

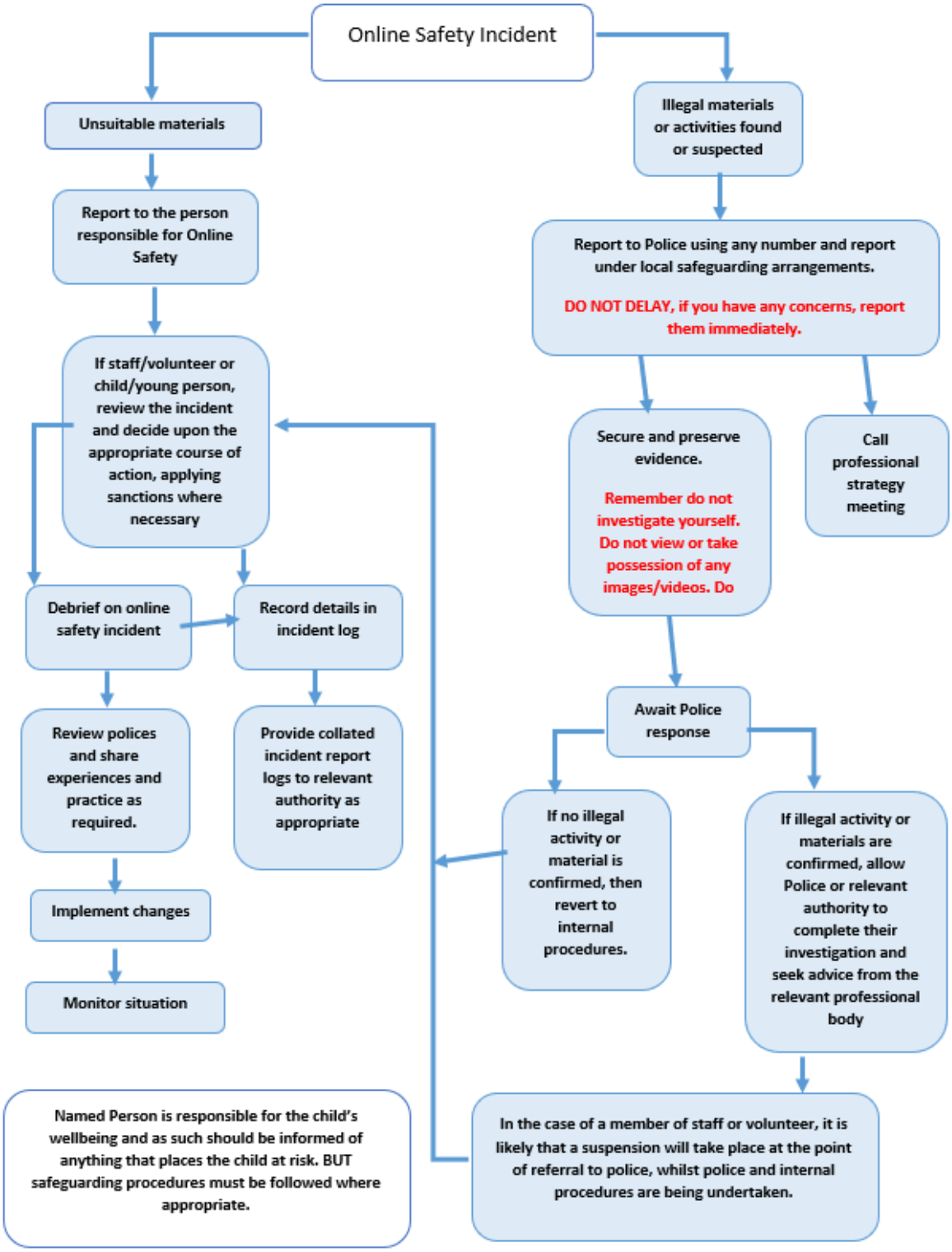
• Using penetration testing equipment (without relevant permission)					
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school/academy				X	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)				X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				X	
Using school systems to run a private business				X	
Infringing copyright				X	
On-line gaming (educational)		X			
On-line gaming (non-educational)		X			
On-line gambling				X	X
On-line shopping/commerce		X			
File sharing		X			
Use of social media		X			
Use of messaging apps		X			
Use of video broadcasting e.g. Youtube		X			

13 Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or unsuitable activities (see "User Actions" Section 12 above).

13.1 Illegal Incidents

131i. If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



13.2 Other Incidents

13.2i It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

13.2ii. In the event of suspicion, all steps in this procedure should be followed:

a. Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
b. The designated computer to be isolated and removed from use to preserve evidence and if necessary taken off site by the police should the need arise.
c. It is important to ensure that the relevant staff should have appropriate internet access to conduct the investigation, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
d. Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used

for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)

e. Once this has been completed and fully investigated a judgement will be made about the nature of this concern. Appropriate action will be required and could include the following:
    i. Internal response or discipline procedures
    ii. Involvement by Local Authority
    iii. Police involvement and/or action
f. If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    i. incidents of 'grooming' behaviour
    ii. the sending of obscene materials to a child
    iii. adult material which potentially breaches the Obscene Publications Act
    iv. criminally racist material
    v. other criminal conduct, activity or materials
    vi. promotion of terrorism or extremism
    vii. offences under the Computer Misuse Act (see User Actions chart above)

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

13.2iii It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. Written evidence should be retained by the group for reference purposes by recording it on the sensitive issues confidential log.

13.3 School Actions & Sanctions

13.3i It is more likely that the school will need to deal with incidents that involve unsuitable 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 the School Behaviour, Child and Data Protection Policies. This includes mobile device use on personal networks whilst at school.

13.3ii In the event of a staff breach of the E-safety Policy, the Headteacher will use the Staff Code of Conduct and Misconduct Policy where appropriate.

Appendix A

14. Student Acceptable Use Policy:

This policy applies to all school devices and for mobile devices used on the school network and private networks whilst on school site.

14.1 Every time a student logs on to a network computer they agree (by clicking the agree button) to the 'Acceptable Use Policy' which provides guidelines to keep them safe online, without restricting their education. Although it is difficult to monitor students' own devices, we have provided a section which encourages them to use their phones, tablets and laptops in a responsible and safe manner.

Student guidelines for use of the Computer Network and the Internet:

It should be remembered at all times that the school computer network is provided for educational purposes and should not be misused on both school and personal mobile devices. All usage of the network and internet is constantly filtered and monitored. Laptops loaned from the school on behalf of the DfE have recently been updated to include the school's online filtering and security. Students signature of this Acceptable Usage Policy reflects their agreement to adhere to the rules outlined below.

When using the Network, internet and school devices, Whitley Bay High School students must:

a. Keep their password safe and never give it to another user;
b. Treat the equipment with care and respect;
c. Not be wasteful of resources – particularly colour printing;
d. Save all work to their personal network area or their cloud through Onedrive – students must not save any data onto external storage devices that could contain sensitive data. USB ports will be disabled from September 2018;
e. Only use devices for curriculum purposes;
f. Report any damage or malfunctions to a member of staff as soon as possible.
g. Use appropriate language in communication

When using the Network, internet and school devices, Whitley Bay High School students must not:

a. Attempt to access/hack into the school network administration
b. Attempt to access/hack into the network areas of other users
c. Attempt to bypass the internet filtering system or any other security features.
d. Knowingly commit any data breaches by publicly sharing the sensitive information of oneself or others. This could include name, address and phone numbers for example.
e. Attempt to access software not assigned to them
f. Knowingly plagiarise any work
g. Attempt to access and share any unsuitable information (offensive, racist, illegal etc)
h. Attempt to download, store or install software to school computers.
i. Engage in activities that waste technical support time and resources.
j. Access, download, create, store or transmit material that; is indecent or obscene, could cause annoyance or offence or anxiety to others, infringes copyright or is unlawful or brings the name of the school in to disrepute

Students' Mobile Devices:

The school permits use of a students device in order to support learning, organisation and in preparation for work. We do acknowledge 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, could access social media, become involved in peer on peer abuse or sexually harass their peers via their mobile and smart technology. This includes sharing indecent images: consensually and non-consensual (often via large chat groups), and view and share pornography and other harmful content as outlined in the Keeping Children Safe in Education 2021 publication.

Students who use their own devices are expected to apply the same Acceptable Use Policy to their device whilst connected to their personal network in school.

When using own devices during school time, students at Whitley Bay High School should:

a. take ownership and responsibility for their equipment and keep it safe; we cannot protect devices from damage or theft
b. treat other students' equipment with care and respect;
c. report to a member of staff if they are concerned about the actions or welfare of themselves or a peer;

Whitley Bay High School students must not:

a. attempt to use own devices to participate in unsuitable behaviour as in conjunction with the Behaviour and Child Protection Policy;
b. attempt to access online materials that are unsuitable for the school, themselves or others;
c. participate in any cyber bullying using social media;
d. pass on unsuitable or confidential information to others;
e. Contact staff on any online platform except the school email address. This includes attempting to become 'friends' with any members of staff on any form of social media
f. perpetrate or participate in online sexual harassment which may be standalone, or part of a wider pattern of sexual harassment and/or sexual violence. This includes:
    a. consensual and non-consensual sharing of nudes and semi-nudes images and/or videos.
    b. taking and sharing nude photographs of U18s which is a criminal offence
    c. sharing of unwanted explicit content
    d. upskirting (which is a criminal offence)
    e. sexualised online bullying
    f. unwanted sexual comments and messages, including, on social media
    g. sexual exploitation; coercion and threats

I have read, understood and agree to comply with the guidelines for use of my own device at Whitley Bay High School. I accept that:

a. this is a privilege and own devices must be used responsibly;
b. the wi-fi used will connect to the Guest network and be subject to the same monitoring and filtering as the any school device.
c. if I do not follow these guidelines, access to own devices in school may be withdrawn on a temporary or permanent basis and further disciplinary action may be taken;
d. proven mis-use of my privately-owned device(s) on school premises will be subject to the same sanctions, via the school Behaviour and Child Protection Policies, as would have been the case had the School's own equipment been involved.
e. I will not take images of pupils and staff unless I have express permission from school staff, along with explicit consent from the individuals photographed and it is for school purposes. I will not distribute any images outside the school network.
f. I will not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community.
g. I will always respect the privacy and ownership of others' work online.
h. I will respect the work and property of others and will not access, copy or remove another user's files without their knowledge and permission.
i. I understand that Whitley Bay High School may monitor my use of their systems and devices.
j. I understand that Whitley Bay High School may recall the device at any time for monitoring purposes.
k. I understand that if the school suspects that I am using their system for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant authorities.
l. I understand that the school has the right to act against me if I behave inappropriately online outside of school, for example, by cyberbullying another student on social media, or posting their personal information without their permission.

I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied, my computer rights revoked, a personal device removed and my parent/guardian contacted.

I agree that if any school equipment is damaged, lost or stolen, I will immediately inform Mr Sherlaw Deputy Headteacher. The school Charging and Remissions Policy (available on the school website) will be applied to any school equipment which is damaged or lost.

I (the pupil) have read, understood and agree to comply with this policy.
I **(the Parent / Guardian) have** read and understand this policy and have discussed it with my child.

Appendix B

14. Staff Acceptable Use Policy (Section E of the Handbook):

This Agreement has been drawn up between Whitley Bay High School Learning Trust and yourself. Please note: In this agreement, the term personal computer can mean any desktop, laptop or tablet computer belonging to Whitley

Bay High School Learning Trust. This agreement applies to usage of this equipment on and off site. It also applies to any personal electronic media device used on the school premises.

Usage

Use of the internet and personal computers by employees of Whitley Bay High School Learning Trust is permitted where such use supports the goals and objectives of the school. However, Whitley Bay High School Learning Trust now has a policy in place for the use of such equipment and the internet whereby staff must ensure that they:

- Use the internet in an acceptable way
- Remember at all times, any personal computers are the property of Whitley Bay High School Learning Trust
- Agree to bring your loaned computer into school immediately to be checked, if requested by the IT Department, or if the agreed loan period has come to an end.
- Save all work to Onedrive, Sharepoint or staff drives using Office 365 or the RDS remote log in to ensure GDPR compliance.
- Understand that using their own device on the network, will result in the same online monitoring as a school device.
- Adhere to the E-Safety and Data Protection Policy to ensure GDPR compliance

Unacceptable usage

Involvement in any of the activities referred to in this policy, whilst on the school network or school computer will be highly likely to result in disciplinary procedures. In particular the following is deemed unacceptable use or behaviour by employees in school or off site:

- visiting internet sites that contain obscene, hateful, pornographic or otherwise illegal material
- using the computer to perpetrate any form of fraud, or software, film or music piracy. These materials include videos and media (such as YouTube and other video/media streaming websites) and music (including MP3s and other music/media files)
- using the internet to send offensive or harassing (including sexual) or inappropriate material to other users, including images of upskirting, nudes and semi-nudes
- downloading commercial software or any copyrighted materials or media belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such license.
- hacking into unauthorised areas
- publishing defamatory and/or knowingly false material about Whitley Bay High School, your colleagues and/or our students on social networking sites, twitter, 'blogs' (online journals), 'wikis' and any online publishing format
- using software or operating systems not provided or licensed by the school
- using school Apple, Android or phone accounts to make payments online
- introducing any form of malicious software into Whitley Bay High School
- saving any documents that contain sensitive data on a non-encrypted personal device
- any serious breach of the Data Protection Policy (available on the Staff area of SharePoint)
- any serious breach of the E-Safety Policy (available on the Staff area of SharePoint)

Home Loan Access

Whitley Bay High School will operate a computer loan system for those who wish to conduct work at home. This is bookable via the Room Booking System available in the Staff area of SharePoint. Laptops or devices can be loaned in 2 possible windows: from Monday lunchtime to Friday lunchtime or Friday lunchtime to Monday lunchtime. Our network and all school devices use Impero security filtering software and Smoothwall which is strongly recommended by North Tyneside Council. This system applies the same filtering and security both on and off site on school operated machines. Staff who use personal computers onsite as part of BYOD should log into the Guest Wi-Fi to ensure the same level of security. BYOD is encouraged, but computers must be setup in the same way as any other school device whilst on site; this will protect the network and ensure safeguarding of all staff and students, whilst allowing GDPR compliance and the back up of work.

Any attempts to remove or bypass this system, or to use the BYOD onsite in an unacceptable way is also in direct violation of this policy and will be deemed as improper use, leading to potential disciplinary procedures for the member of staff.

Whilst loaning a school computer, you should give careful consideration as to who could access it for both safeguarding and GDPR data breaches. In event of a partner or family member accessing inappropriate sites in contravention of this policy you might find it difficult if not impossible to prove that you were not the user – therefore our advice is that you do not allow your school computer to be used by others, or to be used for personal use. Please remember a school device is not a substitute for a family PC, for booking holidays, online shopping and so on; its function is to support research and lesson preparation, report writing and other school related tasks.

Staff Computers/Desktops
You have 4 potential areas to save work in whilst at school or at home. We strongly advise that you save work online via methods 3 and 4, as there is more storage available, and there will be storage limitations applied to the school network. The 4 areas are:

1) In your named documents folder which contains work in your network user account accessible in school.
2) The staff shared/T drive which is available for all staff to view
3) Your personal OneDrive account via Office 365
4) Your SharePoint area via Office 365.

You can access both 1 and 2 off site via the RDS log in which is available via the school website. We strongly advise that you use your OneDrive and SharePoint most frequently as it has more space, is available more easily (via office 365 login) and is reliably backed up.

External Hard drives and Memory Sticks

You should not be saving any documentation, particularly any which contains sensitive data on non encrypted memory sticks and hard drives. School computers will have all USB ports disabled for general use, to protect against GDPR and network breaches.

Emails
To support a healthy work life balance for all, may we ask, where possible, for emails to be sent when necessary, but using the delay function on Outlook to ensure it arrives in the recipient's inbox during the working day. This is to ensure we support each other to maintain a healthy work life balance.

Our intention with this request, is not to remove the flexibility that email provides, but to ensure those in receipt do not feel obligated to return a reply that instant, when the following working day would be perfectly fine.

Any emails which contain sensitive data and are sent outside of whitleybayhighschool.org accounts, should be password protected with the recipient receiving the password in a separate email.

Agreement

All staff who have been granted the privilege to use Whitley Bay High School's personal computers on and off site are required to accept this agreement confirming their understanding and acceptance of this policy.

15. Governors Acceptable Use Policy:

This Agreement has been drawn up between Whitley Bay High School Learning Trust and yourself. Please note: In this agreement, the term personal computer can mean any desktop, laptop or tablet computer belonging to Whitley Bay High School Learning Trust. This agreement applies to usage of this equipment on and off site. It also applies to any BYOD/BYOT personal electronic media device used on the school premises.

Usage

Use of the internet and personal computers by Governors of Whitley Bay High School Learning Trust is permitted where such use supports the goals and objectives of the school. However, Whitley Bay High School Learning Trust now has a policy in place for the use of such equipment and the internet whereby Governors must ensure that they:

• use the internet in an acceptable way,

• remember at all times, any loaned personal computers are the property of Whitley Bay High School Learning Trust

• agree to bring any loaned computer into school immediately to be checked, if requested by the IT Department, or if the agreed loan period has come to an end.

• Save all work related to Whitley Bay High School to Onedrive or Sharepoint to ensure GDPR compliance.

• Understand that using their own device on the network, will result in the same online monitoring and filtering as a school device.

Unacceptable usage

Involvement in any of the activities referred to in this policy, whilst on the school network or school computer will be highly likely to result in disciplinary procedures. In particular the following is deemed unacceptable use or behaviour by employees in school or off site:

• visiting internet sites that contain obscene, hateful, pornographic or otherwise illegal material,

• using the computer to perpetrate any form of fraud, or software, film or music piracy. These materials include videos and media (such as YouTube and other video/media streaming websites) and music (including MP3s and other music/media files.)

• using the internet to send offensive or harassing (including sexual) or inappropriate material to other users, including images of upskirting, nudes and semi-nudes

• downloading commercial software or any copyrighted materials or media belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such license.

• hacking into unauthorised areas,

• publishing defamatory and/or knowingly false material about Whitley Bay High School, your colleagues and/or our students on social networking sites, twitter, 'blogs' (online journals), 'wikis' and any online publishing format,

• using software or operating systems not provided or licensed by the school,

• using school Apple, Android or phone accounts to make payments online,

• introducing any form of malicious software into Whitley Bay High School,

• saving any documents that contain sensitive data on a non-encrypted personal device

• any serious breach of the E-Safety Policy (available on the school website).

Social Media usage

This section has been taken from the school E-safety policy which should be read and followed by all Governors when acting on behalf of the school. Governors should ensure in their own personal social media that:

- No reference should be made in social media to students, parents or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are the responsibility of Governors who we advise to regularly keep up to date.
- They do not assign any pupil as a 'friend'/contact on their social media page, or any former pupil under the age of 18 or within the current academic year is prohibited, and caution should be taken regarding becoming assigned as a 'friend' with children of school age on the roll of another school or ex-students especially where siblings continue to attend the school. In addition, workers should never use, access, or become

assigned as a "friend" of the social media pages of pupils on the roll of the school, or former pupils under the age of 18[2]. If in doubt please seek advice from your Headteacher/Deputy Head in charge of E-Safety.

- The email address used to create the account is personal to them and not the whitleybayhighschool.org business address
- When commenting, uploading or posting links within social media sites, remarks must never be derogatory, offensive, reflect negatively on your professionalism or that of colleagues or have the potential to bring the school into disrepute. Where Governors become aware of such remarks made by others on social media platforms they should refer these immediately to the Headteacher or the Chair of Governors.
- They review the social media sites they participate in when joining the school, ensuring information available publicly about them is accurate and not inappropriate (e.g. photographs that may cause embarrassment to themselves and the school if they are published outside of the site).
- They do not release any confidential information about themselves, the school, its employees, pupils, partners, or other stakeholders within the community.
- They communicate to the Headteacher or DpDSL Esafety lead any occasions when there are social contacts between pupils and workers. For example, where the parent and teacher are part of the same social circle. However, these contacts will be easily recognised and should be made known to the Headteacher or Chair of Governors where there may be implications for the adult and their position within the school setting.
- Any unsuitable material of a safeguarding nature uncovered relating to Governors' activities both on public and private spaces within a social media site is reported to the Headteacher or Chair of Governors, who will determine the appropriate action inclusive of reporting to external agencies.
- They are aware of the effect their actions may have on their image, actions that may cause offence intended or otherwise, as well as that of the school. Information that workers publish/post may be in the public domain for many years.
- They are aware that the Governing Body will not accept any form of bullying or harassment of or by workers engaged by the school, inclusive of that through social media, commonly referred to as "cyber bullying". This may:

- maliciously spreading rumours, lies or gossip
- intimidating or aggressive behaviour
- offensive or threatening comments or content
- posting comments/photos designed to cause offence e.g. deliberately mocking an individual with the intent to harass or humiliate them

Serious breaches and misuse of social media by Governors could amount to gross misconduct and may result in dismissal. The below list constitutes examples of serious breaches but this list is not exhaustive:

- Breach of confidentiality/copyright
- Behaving in a discriminatory, bullying or harassing way towards others.
- Bringing the school or a partner agency into disrepute
- cyberbullying
- Where a criminal offence has taken place
- Unsuitable material that is of a safeguarding nature

External Hard drives and Memory Sticks

Governors should not be saving documentation, particularly any which contains sensitive data related to the school on non-encrypted memory sticks and hard drives. School computers will have all USB ports disabled for general use, to protect against GDPR and network breaches.

Agreement

All Governors who have been granted the privilege to use Whitley Bay High School's personal computers, the school network and the school Office 365, on and off site, are required to accept this agreement confirming their understanding and acceptance of this policy.

Signed: _____

Date: _____