ONLINE SAFETY POLICY

1. Scope

This policy applies to pupils, staff, volunteers, parents and visitors and covers both inside the schools' buildings, within the schools' grounds and wider.

2. Rationale

Online Safety encompasses the use of new technologies, internet and electronic communications such as mobile phones and tablet devices, collaboration tools and social networking. It highlights the need to educate all stakeholders appropriately about the benefits and risks of using technology and provide safeguards and awareness for users to enable them to control their online experience.

- The Internet and use of new technology are essential elements in 21st century life for education, business and social interaction. It has been instrumental in the delivery of remote learning and will play an ever-increasing role in education as we consider the possibility of hybrid learning models.
- The ALP has a duty to provide pupils with the knowledge, skills, values and opportunities to use the Internet to enhance their learning experience.
- Internet use is a part of the curriculum and a necessary tool for staff and pupils. Pupils are encouraged to use it as long as suitable controls are in place including within the remote environment.
- Pupils and staff use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- The school Internet access is designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils are given clear objectives for Internet use, including what is safe, acceptable and appropriate.

As pupils' confidence in the use of technology increases, it becomes more important that we control its use within schools and educate pupils and staff about using it safely outside that environment.

We accept that mobile phones are increasingly being given to pupils by their parents, in order to ensure their safety. Please see Appendix 1 for more guidance.

We acknowledge that increasing numbers of people use **social networking** sites such as Facebook. The use of social networking applications brings opportunities to understand, engage and communicate with audiences in new ways. It is important that we use these technologies effectively and flexibly. However, it is also vital to ensure that we balance this with our reputation and image. It is important to protect those within the Ashington Learning Partnership from allegations and misinterpretations which can arise from the use of social networking sites. Additionally, we have a firm commitment to safeguarding children in all aspects of our work. Please see Appendix 2 for more guidance.

3. Education and Training

An Online Safety training programme is in place for all members of the school community.

Pupils

- The computing curriculum is designed to equip pupils with the knowledge, skills, values and opportunities they need to use the internet safely. Key online safety messages are reinforced as part of a planned programme of assemblies and extra-curricular activities.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Online Safety rules and relevant, up to date signage are posted in all computer suites and highlighted to the pupils at the start of each year.
- Pupils are informed that network and Internet use is monitored and where students are allowed to freely search the internet, staff are vigilant in monitoring the content of the websites the young people visit.

Staff

- All staff receive an annual safeguarding refresher training session which includes updates to Keeping Children Safe In Education pertinent to online safety.
- A programme of safeguarding CPD is planned annually which incorporates online safety training.
- Staff are trained to understand their role and responsibilities with regards to Online Safety; who they should speak to if they are made aware of an Online Safety incident and how they can support pupils with such concerns.
- Staff are aware of the school's monitoring and filtering systems.

Parents

- Parents' attention is drawn to Online Safety in regular publications, on the school website and Facebook.
- Where appropriate, additional training is offered to parents and information updates are sent home on a regular basis.
- Parents know how the school monitors and filters sites etc to ensure that they are suitable and safe to access.

Governors

- Governors are provided with online or face to face Online Safety training as part of their annual safeguarding refresher.

4. Technical Infrastructure

Safety and security of IT systems:

- ICT systems' capacity and security is reviewed regularly.
- Virus protection and operating system updates are applied regularly and automatically. Such automated systems are reviewed regularly.
- All pupils at KS1 and above are provided with a username and secure password; this is in the form of a set username and password managed by the IT Co-coordinator or Infrastructure Manager.
- The domain administrator passwords for each school are written down, put into an envelope and secured in a safe.
- The Infrastructure Manager is responsible for ensuring that software and hardware

audit inventories are up to date and accurate.

Filtration and monitoring

- The Infrastructure Manager works with the DCSF and the Internet Service Provider, to ensure systems to protect pupils are regularly reviewed and improved.
- Changes to filtration requests must be requested via the Infrastructure Manager.
- If any community member (staff, pupils, etc.) discovers an unsuitable site, it must be reported to the Infrastructure Manager, Online Safety Coordinator or the DSL.
- The Online Safety Coordinator and Infrastructure manager regularly check to ensure that the filtering methods selected are appropriate, effective and reasonable, to ensure high quality education, while keeping pupils safe.
- All computers used within the schools and on school-owned devices are monitored using Senso Cloud.
- A weekly summary report is reviewed by the Infrastructure manager and anything that is flagged is passed to the ICT Coordinator to action. There are regular reviews by the Executive Headteacher and designated Senior Leaders.
- Internet usage is monitored on a regular basis, as per the acceptable use Agreement.
- The above apply to remote learning.

Management of ALP VLE, Google systems and other learning environments

For this section, 'systems' refers to the school's Virtual Learning Environment

- Usage of the Systems by pupils and staff is regularly monitored in all areas, in particular message and communication tools and publishing facilities.
- All users are advised on acceptable conduct when using the Systems.
- Only members of the current pupil, staff and governor community have access to the Systems.
- All users are mindful of copyright issues and will only upload appropriate content onto the Systems.
- When community members (staff, pupils, etc.) leave the school their account or rights to specific school areas will be disabled and deleted.
- Where Apps are used, all data including images are kept securely on servers hosted by the app and subject to their own policies.

5. Data Protection

- Personal data is recorded, processed, transferred and made available according to the stipulations under the Data Protection Act 2018 and the Data Protection Policy.
- Pupil and staff personal data is not displayed, physically or electronically, in public areas or areas where visitors or pupils have access.
- Access to the schools' MIS systems are password protected and managed by Northumberland County Council. Staff are instructed to lock computers when they leave them unattended.

6. Published Content

- Appropriate school addresses, e-mail addresses and telephone numbers are published on the school website. Staff or pupils' personal information are not published.
- The designated person has overall editorial responsibility for the school's website and ensures that content is accurate and appropriate.
- See Use of Images Policy.

Publishing pupils' images and work

- Pupils' full names will not be used anywhere on the school website or social media channels in association with photographs. This is permitted on the VLE which is only accessed by approved users within the school community and is monitored.
- Written permission from parents or carers is obtained before photographs of pupils are published on the school website or checked against each school's use of pupil image form or parent/carers acceptable use agreement. See Use of Images Policy.

Communication

- Staff should only use their school email accounts for business purposes. E-mail sent to parents or an external organisation should be written carefully, in the same way as a letter written on school headed paper.
- The forwarding of chain letters or spam is not permitted.
- Personal mobile phones should not be used to contact parents or pupils unless directed by SLT. If this is unavoidable then the school's DSL or ICT Coordinator should be informed promptly. Under no circumstances should pupil phone numbers be stored on personal mobile phones.
- Mobile phones will not be used during lessons or formal school time.
- Normal school sanctions apply to the use of technology (e.g. the sending of abusive or inappropriate text messages).

7. Emerging Technologies

- Emerging technologies are examined for educational benefit and the risks and benefits considered before use in the ALP is allowed.
- Artificial intelligence - use of A.I. is blocked for pupils. Staff exploring the use of this technology in the classroom should liaise with the Infrastructure Manager to ensure this can be monitored and evaluated in terms of educational benefits and potential risks.

8. Responding to Incidents of Misuse

Handling Online Safety incidents

- Incidents and complaints of Internet misuse will be dealt with by the Assistant Heads in conjunction with the Online Safety Coordinator/team. DSL will be informed if necessary
- Any incident or complaint about staff misuse must be referred to the Executive Headteacher and may be referred to the LADO.
- Incidents and complaints of a child protection nature must be dealt with in accordance with current child protection procedures. See the ALP Safeguarding Procedure.
- The ALP has adopted the NCC's procedures for dealing with Online Safety issues (see incident management flowchart Appendix 5).

Cyber-bullying

- Cyber-bullying (along with all forms of bullying) is not tolerated in school. Full details for dealing with bullying incidents are set out in the schools' behaviour policy.
- There are clear procedures in place to support anyone affected by Cyberbullying.
- There are clear procedures in place to investigate incidents or allegations of Cyberbullying. The Police will be contacted if a criminal offence is suspected.
- All incidents of cyber-bullying reported to the school, will be dealt with in accordance with the Behaviour Policy.

Appendices:

1. **Personal Electronic Devices**
2. **Social Networking - Staff**
3. **ALP Social Media Accounts**
4. **Roles & Responsibilities**
5. **Reporting an Online Safety Incident**
6. **AUP - Staff**
7. **AUP - Visitor**
8. **AUP - Pupil**

Relevant Documents

1. **Behaviour Policy**
2. **Anti Bullying Policy**
3. **Uniform Policy**
4. **Staff Code of Conduct & Dress**
5. **Management of Educational Visits Policy**
6. **Use of Images**
7. **Data Protection**
8. **Contractors' Induction Packs**

Created ☐ Reviewed ☐	
Signed: HW/RC	**Name: Heather Walker/Ross Crichton**
Role: Online Safety Team	**Date: September 2024**
Adopted	
Signed: LH	**Name: Louise Hall**
Role: Executive Headteacher	**Date: January 2022** **Reviewed September 2023**

Reviewed Sept 24

- Tightened up reporting procedures
- Removed reference to School360 as not used
- Removed reference to Seesaw as not used
- Incidents of misuse handled by Ass. Heads first

Personal Electronic Devices

Personal electronic devices include, but are not limited to, existing and emerging:

- Mobile communication systems and smart technologies (mobile phones, iPhones, Smartphones, Smartwatches, internet-enabled phones, etc.).
- Personal Digital Assistants (PDA) (Palm organisers, pocket PCs, etc.)
- Handheld entertainment systems (video game consoles, CD players, compact DVD players, MP3 players, iPods, earphones, etc.).
- Portable internet devices (mobile messengers, iPads, etc.).
- Wireless handheld technologies or portable information technology systems (used for word processing, wireless internet access, image capture/recording, sound recording, and information transmitting/receiving/storing, etc.).

Parents/carers should be aware that if their child takes a mobile phone or smart watch to school, we accept no responsibility for replacing lost, stolen or damaged mobile devices either at school, or travelling to and from school.

Pupils are responsible for protecting their own personal information including their phone number.

Any devices that are being used to access data, including emails, are forced to have a strong password set and 2 factor authentication enabled.

Staff may have work email, calendars and documents on mobile devices or tablets subject to level of password protection. Under these circumstances, staff should not share their password with anyone else, nor let them use the device. They should be aware that if they lose the device while it is unlocked then their information is unprotected; suitable care should be taken.

Staff may not use their own personal devices to take any photos or videos of pupils. Refer to Appendix 1 for more information.

1. **Acceptable use**
    1.1. Pupils' mobile devices and smart watches should be switched off and handed in to the school offices for the duration of the school day. Basic activity trackers are allowed in school but are brought in at owners' risk.
    1.2. Staff may use personal devices in non-working times in designated places only. These are the staffroom, offices and reception offices, if no pupils are present. Devices should not be accessed in any other area used by pupils, even if they are not present at that time. The exception to this is SLT, Designated Safeguarding Leads and IT Team who may use school provided numbers or devices in the course of their duties. Staff may only use personal devices for authentication purposes against websites such as CPOMS, SIMS and Google authenticator, when it is not appropriate or possible to use their school iPad.
    1.3. If it is essential for staff to make or receive a personal call within school time, and they have the permission of a senior member of staff, this should take place in a designated place only.
    1.4. Mobile phones will be taken by the Visit Leader on any school trips or events. The Management of School Visits Policy refers.
    1.5. It is recognised that one of the key ways to support children's development, and engage parents in children's learning, is through photographs that record their

children's activities and achievements. We seek permission from parents/carers to take photographs of their children for this purpose, using the school's own devices. See Use of Pupil Images Policy.

2. **Unacceptable use**
    2.1. Unless express permission is granted, mobile devices should not be used to make calls, send SMS messages, iMessages or emails, take photos or use any other applications.
    2.2. Files should not be sent between mobile devices and Bluetooth and WIFI functions should be disabled while on school premises.
    2.3. If pupils fall ill during school hours, they must not use their mobile device to contact home; they should use the agreed procedures.
    2.4. Under no circumstances should mobile devices be taken into examinations.
    2.5. Under no circumstances should mobile devices be used in changing rooms or toilets.
    2.6. Personal laptops, mobile phones or tablets must not be plugged into outlets on school premises without the express permission of the School Business Manager and an up-to-date portable appliance test (PAT).
    2.7. Staff should not use USB drives and should use Google Drive instead. Staff MUST NOT use un-encrypted USB drives.
    2.8. Downloading and accessing inappropriate websites and data on school personal electronic devices is strictly prohibited.
    2.9. Accessing or using the personal data of any pupil or member of staff for non-work related activity is strictly prohibited.
    2.10. Volunteers, visitors and parents/carers may NOT use personal devices in school unless given expressed permission by a member of the SLT. If observed using a phone they may be asked to leave, and reports may be made to the DSL, SLT or the police as appropriate.
    2.11. Staff must not download data onto their personal devices. Data will be kept, used and accessed on Google Drive only.
    3.12 Staff must not store or share data via public file hosting systems such as Dropbox, OneDrive, iCloud etc.

3. **Cyberbullying**
    4.1 At our school, cyber bullying (sending abusive texts, video or photo messages or sharing videos of physical attacks on individuals
    4.2 Sexting (encouraging someone to share inappropriate pictures or videos of themselves and then sending these to other people) is taken seriously.
    4.3 Incidents of cyber bullying will be dealt with as per the Anti-Bullying Policy or Safeguarding Policy, where appropriate.
    4.4 As part of our on-going commitment to the prevention of cyber bullying, regular education and discussion about Online Safety takes place as part of computing and PSHE.

4. **Spot checks**
    4.1. Pupils are required to comply with any request to disable the screen lock function of their phone and show a DSL or member of SLT.

5. **Sanctions**

5.1. The Guidance for Schools on "Screening, Searching and Confiscation" (DfE, July 2022), provides that confiscation is an appropriate disciplinary measure when applied in a reasonable and proportionate way.

	STAFF				PUPIL				VISITOR / VOLUNTEER			
	Allowed	Allowed at certain times	Allowed with consent	Disallowed	Allowed	Allowed at certain times	Allowed with consent	Disallowed	Allowed	Allowed at certain times	Allowed with consent	Disallowed
Mobile phones may be brought into school	✔				✔				✔			
Use of mobile phones in lessons				✔				✔				✔
Use of mobile phones in social time		✔	✔					✔			✔	
Taking photos on **personal** mobile phones / cameras				✔				✔				✔
Taking photos on **school** mobile phones / cameras	✔						✔				✔	
Use of other mobile devices such as tablets or gaming devices		✔						✔				✔
Use of Smartwatches in school	✔							✔				✔

Social Networking - Staff

This relates to social networking outside work. Blogging and accessing social networking sites during work time or using school equipment is not permitted unless a school designated account.

Social networking activities may include, but are not limited to:

- Blogging (writing personal journals to publicly accessible internet pages).
- Online discussion forums, such as netmums.com.
- Collaborative spaces, such as Facebook, TikTok and Instagram.
- Media sharing services.
- 'Micro-blogging' applications, for example Twitter.
- Live streaming services, for example Twitch, Facebook Live
- Image messaging services, for example Snapchat, WhatsApp

Code of Conduct - Social Networking

For employees' own security all communication via social networking sites should be made with the awareness that anything said, shown or received could be made available, intentionally or otherwise, to an audience wider than that originally intended. It is therefore advised that staff **must**:

1. use social networking sites responsibly and ensure that neither their personal/ professional reputation, or the ALP's reputations are compromised by inappropriate postings;
2. not disclose confidential information relating to his/her employment or identify themselves as a representative of the schools;
3. not use the schools' name, logo, or any other published material without written prior permission from the Executive Headteacher. This applies to any published material including the internet or written documentation;
4. not publish their date of birth and home address and be cautious when giving out personal information about themselves which may compromise their personal safety and security. Identity theft is prevalent with criminals using such information to access to your accounts;
5. always make sure that they log out of Facebook etc. after using it;
6. not accept pupils, or former pupils under the age of 18, as friends – personal communication could be considered inappropriate and unprofessional and makes staff vulnerable to allegations. It is illegal for an adult to network, giving their age and status as a child;
7. not associate themselves online with parents/carers of the pupils within the ALP whom they did not know prior to working at the school or in a separate capacity than that of a parent/carer. We recommend that if staff have already established an online association with these persons prior to this code of conduct that they disassociate themselves from them. Staff should inform the Executive Headteacher in writing where family, friends or other legitimate links have pupils in school;
8. Log a CPOMS and alter the online safety team, if they receive messages on his/her social networking profile that they think could be from a pupil. Also, contact the social networking provider so that they can investigate and take the appropriate action if the post is offensive;
9. not place inappropriate photographs on any social network space or post images of pupils in any circumstances;
10. not post indecent remarks or derogatory, defamatory, rude, threatening or inappropriate comments about the ALP, or anyone at or connected with the schools;
11. not make disparaging remarks about their employer/colleagues. Doing this may be deemed as bullying and/or harassment;

12. not disclose any information that is confidential to the school or disclose personal data or information about any individual/colleague/pupil, which could be in breach of the Data Protection Act;
13. not disclose any information about the ALP that is not yet in the public arena;
14. not post any communication or images which links the ALP to any form of illegal conduct or which may damage our reputation, or potentially bring the schools into disrepute;
15. disclose confidential or business-sensitive information or information or images that could compromise the security of the school;
16. avoid using language which could be *deemed as* offensive to others;
17. bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, data protection, Freedom of Information and other legislation;
18. not use social networking for the promotion of personal financial interests, commercial ventures or personal campaigns where connection to the ALP is identifiable and/or that may bring the ALP into disrepute;
19. have the correct privacy and security settings on all social media accounts. Accounts should be set to private. Details on how to do this is within the help section of each social network.
20. any concerns should be raised with the Online Safety Coordinator or DSL.
21. avoid sharing or promoting misinformation that can be deemed as offensive
22. Staff should ensure that they take appropriate security measures when using external social networking sites so that they protect themselves. https://staysafeonline.org/

Potential and Actual Breaches of the Code of Conduct

The ALP does not seek to discourage staff from using social networking sites. However, all staff should be aware that any occasions where services are deemed to have been used inappropriately will be taken seriously.

Any instances of the inappropriate use of social networking sites will be investigated and depending on the seriousness of the allegations, disciplinary action may be taken. The police will be informed of any activity or behaviour for which there are concerns as to its legality.

Appropriate action will be taken as deemed necessary in order to protect the ALP's reputation and that of its staff, parents, Governors, pupils and anyone else directly linked to the school.

ALP Social Media Accounts

Maintaining an online presence is vital for the ALP, not only in terms of keeping the school community up to date with school events, but also in terms of attracting potential enrolment. Having a school website is an essential part of this, but web users must specifically visit the ALP websites regularly to receive this information. By having social networking pages, the school is feeding school information, news and notices directly into the personal news feeds of parents and the wider school community.

Aims

The purpose of having school social media pages is:

- To continue to advance our school information system with information shared via these channels, along with the existing methods of paper notes, text messages, email and the school website.
- To publicise school events and increase awareness about school fundraising.
- To announce any updated information that appears on our school website via Facebook.
- To highlight positive school achievements in a forum where they can be shared by the whole school community.
- To make school announcements in the most timely way.
- To use social media as a means of marketing the school to a wider audience, as parent voice activity has shown that the majority of our parents use social media and have expressed a desire for us to contact them in this way.
- To engage the community that the ALP serves and to act as a key component of our schools' online presence.
- To facilitate communication and networking opportunities between parents, especially those new or prospective.
- To share resources, advice and guidance with parents about particular aspects of education, e.g. Online Safety advice.

Terms of use of ALP Social media channels

- Only users named in the table below may post on the school's behalf though all staff are encouraged to submit information for posting.
- There is a named lead and deputy lead who are responsible for the content on the school's social media pages and will regularly check the security and integrity of the pages.
- Users should not share anything that may compromise the safety of any member of the school community and never transmit any personal information of pupils, parents or staff.
- Users should not post anything that could be deemed offensive, inappropriate or harmful. Comments or content that are deemed inappropriate will be removed immediately and investigated in line with the staff code of conduct.
- Users should not share any information that is confidential.
- Users cannot tag photographs of children on the page.
- Any photos or videos will only be posted in accordance with the ALP Use of Images Policy.
- Users should not engage in conversation with anyone on social media pages. If there is a question or comment that is deemed to need a response, they should be directed to email or ring the school.
- Facebook Messenger service will be turned off and no correspondence should be private
- Users should not be negative on any posts. The tone of any post should be positive and respectful.
- Any inappropriate comments or activity by parents or other persons will be dealt with in the same manner as if it was face-to-face.

- Users cannot advertise products and services on our schools social media pages.
- Users should post regularly to keep users interested and to reach a wider audience. Where possible use an image or video as a visual post for greater engagement.
- Facebook has a minimum age of 13 and all parents should be reminded that children under the age of 13 should not be on Facebook.
- Users should always remember to consider safeguarding, child protection and data protection policies before posting.
- **Staff have been directed to not 'like' or 'follow' posts on the schools' social media accounts.**

Role
Infrastructure Manager
Executive Headteacher
Business Manager HR and Operations
Cian creative PR
Deputy and Asst Heads
IT & Online Safety Coordinator
IT Technician
Designated Admin

Roles and Responsibilities

The Executive Headteacher has overall responsibility for the safety of the school community. This will then be delegated, as appropriate, to other specific members of staff including the Online Safety Coordinator and the Online Safety Team.

The Assistant Heads of Schools are responsible for the day-to-day implementation and management of these procedures.

Online Safety Coordinator/Group

- Ensure the leadership team is aware of the procedures that need to be followed in the event of an Online Safety incident occurring.
- Provide a "first port of call" service for any Online Safety concerns or incidents.
- Keep up to date with changes to Online Safety and any relevant technologies with a view to presenting them at Online Safety Group meetings.
- Provide training for staff and parents in accordance with the Online Safety Operating Procedures.
- Provide Online Safety curriculum content throughout the year for all key stages.
- Support the curriculum and teachers in delivering Online Safety content throughout the year.
- Provide cross-curricular Online Safety content for other subjects.
- Ensure that staff, visitors and pupils have signed Acceptable Use agreements.

Designated Safeguarding Lead & Deputy DSL's (Members of the Online Safety Group)

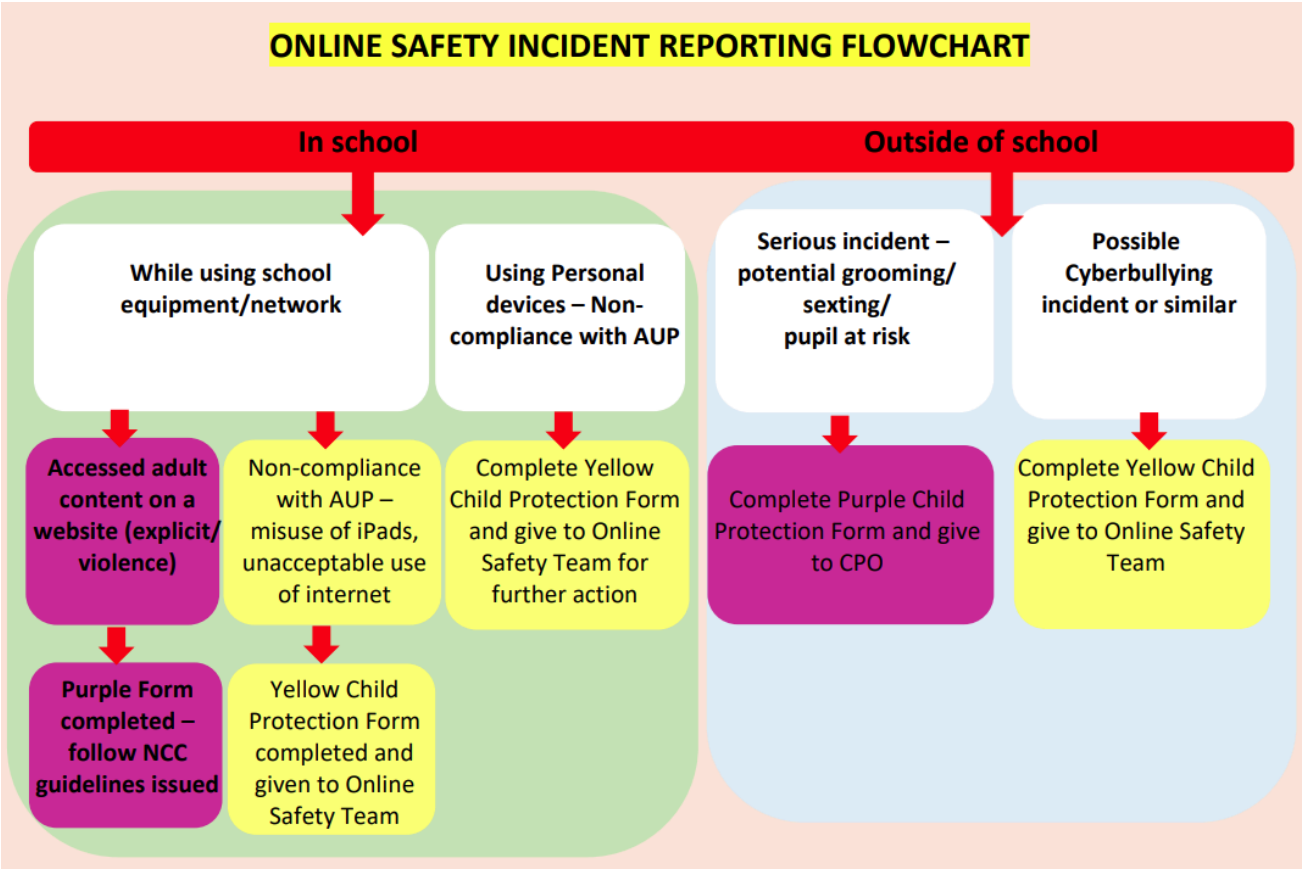
- Take responsibility for dealing with Online Safety incidents which lead to child protection issues. Seek support from Online Safety Coordinator, leadership teams and the local authority where necessary.
- Keep up to date with this Online Safety Policy and have a working knowledge and understanding of the other associated policies.
- Contribute to the review of Online Safety polices in light of any changes to safeguarding policies or procedures.

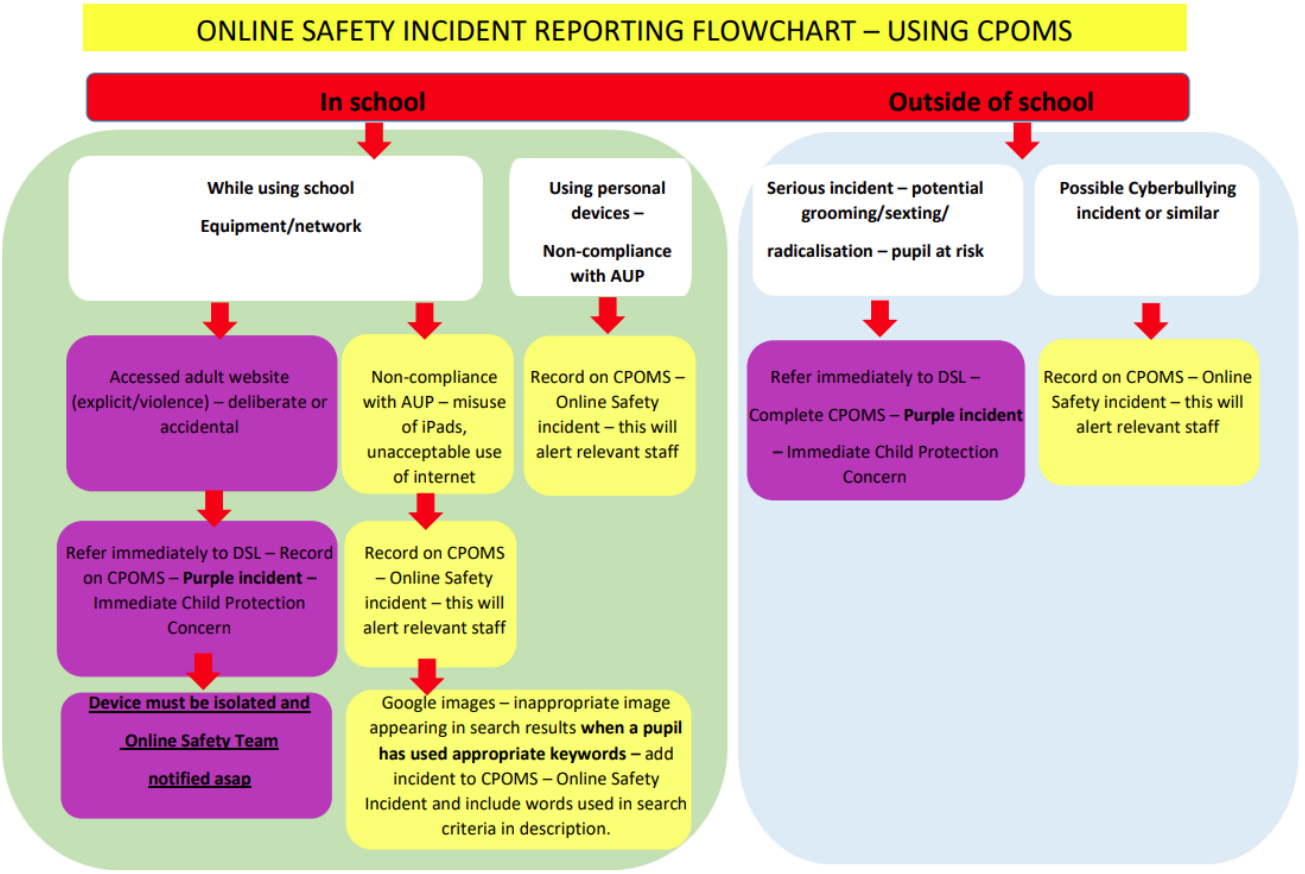
Online Safety/Safeguarding Governor

- Annual meeting to scrutinise Online Safety provision.
- Complete online training for Online Safety as appropriate.

Everyone in the ALP has a responsibility to ensure that they protect the reputation of the schools, and to treat colleagues and members of the school with professionalism and respect.

E-Safety Flow Chart





Appendix 6

STAFF ICT ACCEPTABLE USE AGREEMENT

Introduction

This Acceptable Use Agreement is intended to ensure:

- That users will be responsible and stay safe whilst using ICT for educational, personal and recreational use.
- That ICT equipment and users are protected from accidental or deliberate misuse.

The IT Department will do its utmost to ensure that users have good access to ICT and in return, users must accept responsibility for their actions.

Agreement

Users are responsible for using ICT systems and equipment in an appropriate, safe and secure manner.

- All use of ICT will be monitored by the Infrastructure Manager. Ensure that you use such devices in an appropriate manner; your internet usage here is your own responsibility.
- Your user account and password are confidential. You must not allow other users to access your account and you must not attempt to access any other account. Use of a student's account is acceptable whilst the student is present or the reason is appropriate, i.e. to aid the students' learning.
- You must immediately report any misuse, inappropriate material or messages to the Infrastructure Manager.
- The ICT systems are provided primarily for educational and professional use. You may only use the organisation's ICT systems or equipment for personal use if doing so does not compromise your ability to do your job in its fullest capacity.
- Without consent, you must not attempt to access, download, transfer or stream large files (such as videos longer than 2 minutes or files over 100Mb) which may have a detrimental impact on the network and thus other users' experience of the ICT systems.

The Infrastructure Manager has a responsibility to maintain the security of the technology it offers its users and to ensure the smooth running of its network and all ICT systems and equipment.

- You must not try to upload, download or access any materials which are illegal or inappropriate.
- You must not try in any way, to bypass any of the security systems on the network or ICT equipment.
- You must immediately report any damage or faults to equipment or software, Online Safety concerns or suspected security weaknesses.
- You must not open any email attachments or links in emails, unless you know and trust the sender of the email, due to the risk of the attachment/website containing viruses or other harmful programs.
- You must not attempt to install or store software on any ICT equipment. All software to be used on the ICT equipment must be installed by the IT Department and licensed to the school. Any new software which doesn't require installation, i.e. software run from a flash drive, must only be done so with consent.
- You must not attempt to alter settings on any ICT equipment without consent.
- You must not attempt to download, store or reproduce data protected by copyright (including but not limited to music, videos and any YouTube clips which have been downloaded rather than streamed).
- You must not take or publish images or video recordings of others without permission and in accordance with the organisation's policy on the use of such media. Without consent you must not use any personal device for taking photographs or recording videos.

Users are solely responsible for use of personal devices whilst representing the organisation.

- You must only use personal devices in accordance with the schools Online Safety Policy and this Acceptable Use Agreement.
- You must ensure that any personal devices are physically secure when on the premises of the organisation or in a public environment. This means the device should be either on your person or securely locked away.
- If your personal device is setup to access your organisational email account, the device must be secured with a 8 digit (or longer) PIN code or password, or it must be encrypted by the IT Department as well as having 2 factor authentication enabled
- When using a non-school device to access your work emails or Google accounts, they should be logged out after use and usernames or passwords not remembered on the device. No documents should be downloaded from Google Drive onto a non-school device

- Your personal device should not be used by anyone other than yourself.

Each user is responsible for designated equipment and its use in accordance with the organisation's Online Safety Policy and this Acceptable Use Agreement.

- Designated equipment may be signed out to you to assist in completion of your job role. This could take the form of a laptop, mobile phone or any other equipment as seen fit by the organisation's senior leaders. The equipment remains the property of the organisation and as such should be used in accordance with this Acceptable Use Agreement.
- You must ensure that designated equipment is physically secured. This means any devices should be either on your person or securely locked away.
- Designated equipment is covered by the organisation's insurance while it is on the organisation's premises and in your home. However, users should note that it is NOT insured if left unattended in a car or other vehicle.
- You must look after and protect the equipment from theft or damage, and are expected to report all incidents of theft or damage to the IT Department within 24 hours.
- Internet access on designated equipment outside of the organisation continues to be monitored by the Infrastructure Manager but the organisation is unable to provide filtration services away from its premises. As such you are expected to monitor internet usage and ensure that it is safe and appropriate.
- Files and data stored on your personal or shared Google Drive areas will be backed up by the Infrastructure Manager. Personal Drives will only be kept for 30 days before permanently being deleted. You acknowledge that we are unable to back data up when stored elsewhere (e.g. the local hard drive or memory sticks). You accept responsibility for ensuring this data is backed up.

Each user is responsible for the protection of data in accordance with the organisation's Data Protection Policy:

- As a member of staff within the organisation, you share responsibility for protecting the integrity and security of any data handled using the organisation's ICT equipment.
- Whilst it is desirable not to need to remove data from the organisation's premises, this may on occasion be necessary. You accept responsibility for ensuring this data is stored, transported and handled only on encrypted or password protected media as per the policy. This includes designated equipment such as memory sticks and staff laptops. The IT Department can encrypt memory sticks, external hard drives and other devices so please discuss your requirements with them before attempting to move data off premises.
- Users should be aware that email is not a secure and encrypted method of sending confidential data.

Users are responsible for actions regardless of whether or not they are on the organisation's premises:

- If you fail to follow the rules outlined in this Acceptable Use Agreement, you may be subject to disciplinary action. In the event of any illegal activities the organisation may involve the Police and Local Authority.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement.

I confirm that I have read and understand the ALP Online Safety Policy and Code of Conduct. I agree to follow the guidelines set out by the Acceptable Use agreement guidelines when:

- I use ICT systems and equipment, regardless of time or location.
- I use designated equipment, regardless of time or location.
- I use personal devices at work, or elsewhere if the devices are being used for work purposes (i.e. accessing the organisation's ICT systems such as e-mail or VLE).

Please sign and return to the office.

I agree to abide by the rules set out in this Acceptable Use Agreement.

Signed: Print name: Date:

……

Appendix 7

VISITOR ICT ACCEPTABLE USE AGREEMENT

Introduction

This Acceptable Use Agreement is intended to ensure:

- That users will be responsible and stay safe while using ICT for educational, personal and recreational use.
- That ICT equipment and users are protected from accidental or deliberate misuse.

The IT Department will do its utmost to ensure that users have good access to ICT and in return, users must accept responsibility for their actions.

Agreement

Users are responsible for using ICT systems and equipment in an appropriate, safe and secure manner.

- All use of ICT will be monitored by the Infrastructure Manager.
- You must use any personal devices in accordance with this Acceptable Use agreement.
- If you are provided with a user account and password to access the Infrastructure, these are confidential. You must not allow other users to access your account and you must not attempt to access any other account.
- You must immediately report any misuse, inappropriate material or messages to the Infrastructure Manager.
- The ICT systems are provided primarily for educational and professional use. You may only use the organisation's ICT systems or equipment for personal use when given consent.
- Without consent you must not attempt to access, download, transfer or stream large files (such as videos longer than 2 minutes or files over 100Mb) which may have a detrimental impact on the Infrastructure and thus other users' experience of the ICT systems.

The Infrastructure Manager has a responsibility to maintain the security of the technology it offers its users and to ensure the smooth running of its Infrastructure and all ICT systems and equipment.

- You must not try to upload, download or access any materials which are illegal or inappropriate.
- You must not try in any way to bypass any of the security systems on the Infrastructure or ICT equipment.
- You must immediately report any damage or faults to equipment or software, Online Safety concerns or suspected security weaknesses.
- You must not open any email attachments or links in emails, unless you know and trust the sender of the e-mail, due to the risk of the attachment/website containing viruses or other harmful programs.
- You must not attempt to install or store software on any ICT equipment. All software to be used on the ICT equipment must be installed by the IT Department and licensed to the school. Any new software which doesn't require installation, i.e. software run from a flash drive, must only be done so with consent.
- You must not attempt to alter settings on any ICT equipment without consent.
- You must not attempt to download, store or reproduce data protected by copyright (including but not limited to music, videos and any YouTube clips which have been downloaded rather than streamed).
- You must not take or publish images or video recordings of others without permission and in accordance with the organisation's policy on the use of such media.
- You must not use any personal device for taking photographs or recording videos.

Users are solely responsible for use of personal devices whilst representing the organisation.

- You must only use personal devices in accordance with the schools Online Safety Policy, Personal Electronic Devices

Policy and this Acceptable Use Agreement.

- You must ensure that any personal devices are physically secure when on the premises of the organisation or in a public environment. This means the device should be either on your person or securely locked away.
- Your personal device should not be used by anyone other than yourself.

Each user is responsible for designated equipment and its use, in accordance with the organisation's Online Safety Policy and this Acceptable Use Agreement.

- Designated equipment may be signed out to you to assist you in your visiting role. This could take the form of a laptop, mobile phone or any other equipment as seen fit by the organisation's senior leaders. The equipment remains the property of the organisation and as such should be used in accordance with this Acceptable Use Agreement.
- You must ensure that designated equipment is physically secured. This means any devices should be either on your person or securely locked away.
- Designated equipment must not be taken away from the organisation's premises without consent.
- You must look after and protect the equipment from theft or damage, and are expected to report all incidents of theft or damage to the IT Department within 24 hours.
- Unless specifically requested and sanctioned by the Infrastructure Manager, designated equipment offers no form of backed-up storage. You accept responsibility for ensuring your data is backed up.

Each user is responsible for the protection of data in accordance with the organisation's Data Protection Policy:

- As a signatory of this Acceptable Use Agreement, you share responsibility for protecting the integrity and security of any data handled using the organisation's ICT equipment.
- Users should be aware that email is not a secure and encrypted method of sending confidential data.

Users are responsible for actions regardless of whether or not they are on the organisation's premises:

- If you fail to follow the rules outlined in this Acceptable Use Agreement, your access privileges to the ICT systems, Infrastructure and any designated equipment will be revoked. In the event of any illegal activities, the organisation may involve the Police and Local Authority.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement.

I confirm that I have read and understood the ALP School Online Safety Policy and Code of Conduct. I agree to follow the guidelines set out by the Acceptable Use Agreement guidelines when:

- I use ICT systems and equipment, regardless of time or location.
- I use designated equipment, regardless of time or location.

Please sign and return to the Office.

I agree to abide by the rules set out in this Acceptable Use Agreement.

Signed: Print name: Date:

…….. ……..

Appendix 8

PUPIL ICT ACCEPTABLE USE

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers / tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer / tablet
- I will make sure that all ICT contact with other children and adults is responsible, respectful and sensible.
- I will not deliberately look for, save or send anything that could be upsetting or not allowed at school. If I accidentally find anything like this, I will close the screen and tell a teacher immediately
- I will not give out my own details such as my name, phone number or home address.
- I will hand my mobile phone in at the start of school. I will not use my mobile phone while on the school premises, including after school clubs or events, or during any school trips or visits away from the premises at any time.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I know that the school may check my use of ICT and monitor the Internet sites I have visited, and that my parent/carer will be contacted if a member of school staff is concerned about my Online Safety.