AAT IT Acceptable Use & Online Safety (Including Online Safety Acceptable Use Agreements) Policy

Last Reviewed	March 2024
Reviewed by	Trust Board
Date of Approval	
Lead responsibility	Director of IT
Next Review	March 2025

	IT – Acceptable Use & Online Safety (Including Online Safety Acceptable Use Agreements)	
Alban Academies Trust	**Last reviewed:** March 2024	**Next Review:** March 2025

1. PRINCIPLES

Alban Academies Trust (AAT) takes pride in pioneering innovative approaches to learning, including many of our schools embracing a blended learning approach where students are equipped with personal devices.

Teachers and other student-facing members of staff may be issued with laptop computers and tablet devices for teaching purposes.

The AAT recognises that internet, mobile and digital technologies provide positive opportunities for children and young people to learn, socialise and play but they also need to understand the challenges and risks. The digital world is an amazing place, but with few rules. It is vast and fast moving and young people's future economic success may be partly dependent on their online skills and reputation. We are, therefore, committed to ensuring that all children and young people, staff, governors and Trustees will be supported to use internet, mobile and digital technologies safely. This is part of our safeguarding responsibility. Staff are aware that some children and young people may require additional support or teaching, including reminders, prompts and further explanation to reinforce their knowledge and understanding of online safety issues.

The AAT is also committed to ensuring that all those who work within the Trust with children and young people, including their parents/carers, are informed about the ever-changing risks so that they can take an active part in helping children and young people navigate the online world safely and confidently.

2. TRUST ARRANGEMENTS

This policy outlines the acceptable use procedures across our Trust schools for use of

- IT equipment provided to staff by the schools
- School network etiquette and privacy

AAT Schools will all adopt the **AAT IT Acceptable Use and Online Safety Policy** (based on the model policy provided by Herts for Learning). Please see the Acceptable Usage Section below for this policy.

It is essential that all staff within the Trust read this document and adhere to the terms and conditions.

3. ROLES AND RESPONSIBILITIES

The headteacher and governors have ultimate responsibility to ensure that appropriate online safety policy and practice is embedded and monitored. Each school will appoint a relevant member of staff who will be delegated and responsible for online safety.

All breaches of this policy must be reported to the member of staff within the school responsible for online safety.

All breaches of this policy that may have put a child at risk must also be reported to the school's DSL.

Organisations that are renting space from the school and are a totally separate organisation should have and follow their own online safety policy and acceptable use agreements. However, if the organisation has any access to the school network, cloud-based services and/or equipment then they must adhere to the school's online safety procedures and acceptable use agreements.

If the organisation is operating in school time or when children and young people are on site in the care of the school, then the safeguarding of children and young people is paramount and the organisation must adhere to the school's online safety procedures and acceptable use agreements.

3.1 Board of Trustees

The Board of Trustees are responsible for the approval of the **AAT IT Acceptable Use and Online Safety Policy**. The Trust safeguarding trustee is responsible for reviewing the effectiveness of the policy. This will be carried out by receiving regular information about online safeguarding incidents and monitoring reports.

3.2 Local Governing Body

Governors are responsible for the approval of the **AAT IT Acceptable Use and Online Safety Policy** and for reviewing the effectiveness of the policy. The role of safeguarding governor will include responsibility for Online Safety, which includes:

- regular meetings with the Online Safety Lead
- regularly receiving (collated and anonymised) reports of online safety incidents
- checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training is taking place as intended)
- reporting to relevant governors group/meeting
- occasional review of the filtering change control logs and the monitoring of filtering logs
- asking the questions posed in the UKCIS document "Online Safety in Schools and Colleges – questions from the Governing Body"

3.3 Headteachers and Senior Leaders

AAT headteachers have a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety may be delegated to the Online Safety Lead.

The headteacher and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (See flow chart on dealing with Online Safeguarding incidents – included in a later section – "Responding to incidents of misuse" and relevant Trust disciplinary procedures).

The headteacher/senior leaders are responsible for ensuring that the Online Safety Lead, technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.

3.4 Online Safety Lead

Each AAT school has an Online Safety Lead. Their responsibilities include:

- take day-to-day responsibility for online safety issues, being aware of the potential for serious child protection concerns
- have a leading role in reviewing the school online safety policy
- promote an awareness of and commitment to online safety education / awareness raising across the school and beyond
- liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents

- receive reports of online safety incidents and create a log of incidents to inform future online safety developments
- meet regularly with the safeguarding governor to discuss current issues, review (anonymised) incidents and if possible, filtering and monitoring logs
- provide half termly reports for the Governing body and Trustees
- liaises with the AAT Director of IT and AAT Trust Safeguarding Lead.

3.5 AAT IT

The central AAT IT Team including school Network Managers/Technicians/Technical staff[1] with technical responsibilities are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required online safety technical requirements
- that users may only access the networks and devices through a properly enforced password protection policy
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher, Senior Leaders and the member of staff responsible for online safety within the school.
- that monitoring software/systems are implemented and updated as agreed in school policies

3.6 School Designated Safeguarding Lead

The schools' Designated Safeguarding Lead (DSL)/Designated Person/Officer should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- online-bullying

3.7 Teaching and Support Staff

Trust and school staff are responsible for ensuring that:

- they have an awareness of online safety matters and of the current school Online Safety Policy and practices
- they have read, understood, and signed the staff acceptable use agreement (AUA)
- they immediately report any suspected misuse or problem to (insert relevant person) for investigation/action, in line with the school safeguarding procedures
- all digital communications with learners and parents/carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure learners understand and follow the Online Safety Policy and acceptable use agreements
- they monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices

[1] If the school has a managed ICT service provided by an outside contractor, it is the responsibility of the school to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the AAT technical staff. It is also important that the managed service provider is fully aware of the school online safety policy and procedures.

- in lessons where internet use is pre-planned learners should be guided to sites checked as suitable for their use
- have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

3.8 Learners

- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement (*see **Appendix D & E***)
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should know what to do if they or someone they know feels vulnerable when using online technology
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the Trust's Online Safety Policy covers their actions out of school, if related to their membership of the school.

3.9 Parents and Carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way. AAT schools will take every opportunity to help parents and carers understand these issues through:

- publishing the school Online Safety Policy on the school website
- providing them with a copy of the learners' acceptable use agreement (*see **Appendix D & E***)

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

- reinforcing the online safety messages provided to learners in school
- the use of their children's personal devices in the school

3.10 Community Users

Community users that are renting space from the school and are a totally separate organisation should have and follow their own online safety policy and acceptable use agreements. However, if the community users have any access to the school network, cloud-based services and/or equipment then they must adhere to the Trust's online safety procedures and the schools' acceptable use agreements.

If the community users are operating in school time or when children and young people are on site in the care of the school, then the safeguarding of children and young people is paramount and the organisation must adhere to the Trust's online safety procedures and the schools' acceptable use agreements.

4. DEFINITIONS

IT Equipment – to include all hardware used within schools that are linked to the network including portable devices such as, but not limited to, laptops, digital cameras, tablets.

Network Support – staff who support the use of IT equipment and systems.

5. ACCEPTABLE USE OF IT EQUIPMENT

All members of the school community will be asked to sign a relevant Acceptable Use Agreement, as set out in the appendixes of this policy.

5.1 Communication

When using communication technologies, all schools in the Trust consider the following as good practice:

- when communicating in a professional capacity, staff will ensure that the technologies they use are officially sanctioned by the school
- any digital communication between staff and learners or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content. Personal e-mail addresses, text messaging or social media must not be used for these communications.
- staff are expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community
- users should immediately report to a nominated person – in accordance with the 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
- relevant policies and permissions should be followed when posting information online e.g., school website and social media. Only school e-mail addresses should be used to identify members of staff and learners.

All learners and users are expected to abide by the generally accepted rules of network etiquette. These rules include, but are not limited to the following:

- BE POLITE. Never send or encourage others to send abusive messages
- USE APPROPRIATE LANGUAGE. Remember that both members of staff and learners are representatives of the school and trust on a global public system. An individual may be alone with their computer, but what is said and done can be viewed by others. Staff and learners should never swear, use vulgarities or any other inappropriate language. Illegal activities of any kind are strictly forbidden
- PRIVACY. Staff should not reveal any personal information to anyone, especially the home address or personal telephone of themselves or details of learners
- PASSWORD. Staff and learners should not reveal their password to anyone. If they believe that someone has obtained their password, they should contact a member of the Network Support department immediately and change their password
- EMAIL. Should not be private between staff and learners. Staff and learners should NEVER communicate with each other via their personal email account. Staff should use their school email account to communicate with learners and parents, since an audit trail is kept of these messages. This is for their own and learner safety.
- PROOFREAD messages to ensure that it is error free and easy to understand
- SHARING. Resources can now be easily shared electronically with learners via, but not limited to, Google Drive and Classroom. It is the member of staff's responsibility to ensure that the information shared with learners is appropriate and limited to that which is needed to support their learning and via a platform/system/app approved by the AAT Director of IT and the Network Support department. Staff should show caution when inviting learner groups to share digital content and ensure that nothing confidential or private is shared with learners.

5.2 Internet

With use of school technology and the internet comes the responsibility of the user to only access materials that are considered appropriate, inoffensive and legal. To ensure this, the AAT reserves the right to scan portable devices without notice and check for inappropriate or offensive material. Likewise, users should have no assumption of privacy in using any school's internet service or email services which may be monitored or accessed during any investigation.

5.3 IT Equipment

With home use of school technology comes the responsibility of the user to only access materials that are considered appropriate, inoffensive and legal. To ensure this, the AAT reserves the right to scan portable devices without notice and check for inappropriate or offensive material. Likewise, staff

should have no assumption of privacy in using any school's internet service or email services which may be monitored or accessed during any investigation. When deciding whether or not to examine an electronic device owned by a pupil, school staff will follow the DfE guidance document 'Searching, screening and confiscation: Advice for headteachers, school staff and governing bodies'. This guidance will also be followed when making decisions about how the data and files on a searched electronic device will be managed.

Members of staff employed by the AAT may be issued with several important items of loaned equipment for which staff will be responsible. These may include a laptop and associated materials (cables and power adapter, carrying case or sleeve etc.) Teaching staff and some other student-facing staff have the option to be issued a tablet device (Apple iPad or Android device) and charging cable. Staff may also borrow other technical equipment such as but not limited to iPads, digital cameras, voice recorders and external storage devices. To qualify, staff must read, sign and accept the staff responsibility agreement (*see* ***Appendix A***) that will be given to staff on receipt of equipment from the Network Support team.

The Acceptable Use Policy also applies to personal devices brought onto school premises by staff and visitors. Whilst staff and visitors are welcome to connect their own devices to the school WIFI network, the same rules around content and usage apply (e.g. staff member using personal mobile phone to tweet about a school event).

6. TERMS AND CONDITIONS OF THE ACCEPTABLE USE AGREEMENT – IT EQUIPMENT

Misuse may come in many forms, but it is commonly viewed as any message(s) sent or received that indicate or suggest pornography, unethical or illegal requests, racism, sexism, inappropriate language, any use which may be likely to cause offence and other issues described below. Listed below are the provisions of this agreement. If any member of staff violates these provisions, access to their laptop and other devices will be denied and the staff member will be subject to an investigation and possible disciplinary action. The e-mail, Google Drive and network accounts of the member of staff will be locked during this investigation.

6.1 Personal Responsibility

The items remain the property of the AAT school that issues the equipment and are for use ONLY by the named member of staff. Staff members should not use items for any purpose which would contravene reasonable expectations for the conduct of an employee of the Trust. Items purchased by the AAT school and loaned are to be used to further the educational goals of the school. It is not, for instance, appropriate for school iPads to remain at home to be used by children of staff. If an item of personal technology that has been loaned is no longer needed, staff are expected to return it to the Network Support Department[2] based in their school.

6.2 Acceptable use of equipment

The use of electronic services and technology must be in support of education, administration and research in accordance with the educational goals and objectives of the issuing AAT school. Staff are personally responsible for this provision at all times when using the electronic information service and technology. Use of other networks or computing resources must comply with the rules appropriate to that network. Transmission or use of any material in violation of any United Kingdom or other national laws are prohibited. This includes, but is not limited to, copyrighted material, threatening or obscene material or material protected by trade laws. Personal uses for matters unrelated to teaching & learning within the laws of the United Kingdom outside of school hours are permitted.

[2] For schools with no Network Support staff onsite please return to IT contact within the home school

6.3 Privileges
The use of the Internet and other electronic technology is a privilege and inappropriate use will result in that privilege being withdrawn. Given how fundamental these systems are to our schools' teaching and learning approach, this would have serious ramifications for teaching staff in limiting their ability to discharge their responsibilities.

6.4 Social Media and online communications
The increasing popularity of social media in recent years has allowed many teachers to enhance their classroom practice, introducing their children and young people to new tools and delivering the curriculum in innovative and engaging ways. This is positively encouraged through staff CPD such as Teaching Tips, Twilight INSET and the school websites. However, there are many potential challenges and ramifications in using social media that staff should be aware of as a teaching professional, and appropriate boundaries must be observed between a 'professional' online presence and personal use of social media services.

Reference to online communications and social media include software, applications (including those running on mobile devices), email and websites, which enable users to interact, create and exchange information online. Examples include, but are not limited to, sites such as Facebook, Twitter, LinkedIn, YouTube, Wikipedia and Instagram. Also included is the use of SMS and instant messaging clients, such as WhatsApp, iMessage and Snapchat.

A teacher can be vulnerable to unintended misuses for electronic communication. E-mail, texting and social media encourage casual dialogue and often innocent actions can easily be misconstrued or manipulated.

Electronic messages are not anonymous and can be tracked and live forever on the Internet. Social Media sites archive content posted, even when deleted from online profiles. Once information is placed online, the author relinquishes control of it. A teacher should never share information with children or young people in ANY environment that they would not willingly or appropriately share in a school or school-related setting or in the community.

The following examples would be considered to be a breach of AAT policy:
- inappropriate electronic communication with children and young people, colleagues and parents/carers, including SMS and instant messaging;
- posting/sending sexually explicit pictures/images to colleagues or children and young people;
- grooming - whereby a teacher uses electronic messages with a view to establishing an inappropriate relationship with a pupil;
- possessing, making, viewing or distributing indecent images of children;
- using inappropriate YouTube content in the educational setting;
- posting content that could bring the profession, the AAT or the school into disrepute;
- linking to, 'liking', 'retweeting' or otherwise endorsing content that contravenes the school's policies on discrimination and the upholding of tolerance and respect, appropriate for an education professional.

6.4.1 Social media platforms
There is a proliferation of social media platforms, many of which are very popular with our children or young people e.g. Instagram, Snapchat, WhatsApp etc. The **AAT Social Media Policy** should be followed by all staff when using social media. Staff are entitled to have a personal presence on social media platforms, but should observe at all times appropriate conduct commensurate with their professional standing and their child safeguarding responsibilities.

6.5 Services
The AAT makes no warranties of any kind whether expressed or implied, for the network service it is providing across all of the schools. The AAT will not be responsible for any damages suffered whilst on these systems. These damages include loss of data as a result of delays, non-deliveries, mis-deliveries or service interruptions caused by the system or elements of the system, or staff errors or omissions. Use of any information obtained via any of the schools' network or other information systems is at the member of staff's own risk. The AAT specifically denies any responsibility for the accuracy of information obtained via its Internet services.

6.6 Security of Equipment
Staff are expected to ensure that any equipment provided such as a laptop and other accessories will be kept securely at all times and recognise that if it is lost, damaged or stolen due to a lapse in personal security, staff may be liable for replacing or repairing the device. To ensure security, portable devices and technology should be stored in the boot of cars when in transit or when leaving the device in the car when parked. At home, the device should be stored away from direct sunlight and view of passersby. To ensure security at school, the device should be stored in a secure location, particularly when it will be unattended for a period of time. Staff are responsible for reading and adhering to all Health & Safety and Care literature provided with their portable device. The laptop computer is insured under school insurance policy on the condition that all reasonable precautions should be taken to ensure the security of the equipment and the (sometimes sensitive and confidential) data held on it. It is not reasonable to leave the item in an unattended vehicle or in an unlocked room in school.

If staff are found to be negligent they will be required to pay for a replacement of the item lost or damaged. The costs of repair due to damage caused by negligence (for example, transporting a laptop around the school without a case/sleeve) will also be borne by the staff member. A new laptop will cost approximately £400.

Further information and guidelines regarding the security of equipment can be found within the **AAT ICT & Cyber Security Policy.**

6.7 Security of Data
All teaching staff and some support staff are in possession of confidential, sensitive and personal data about children and parents/carers and we all have an explicit duty under law to guard this data and use it appropriately.

The AAT takes the security of information very seriously and recognises our duties under the new General Data Protection Regulations of 2018. Please see the **AAT GDPR Policy** and individual schools' Data Security Policies for further guidance.

Further information and guidelines regarding security of data can be found within the **AAT ICT & Cyber Security Policy.**

6.8 Vandalism
Vandalism is defined as any malicious attempt to harm or destroy any equipment or data of another user or of any other networks that are connected to the system. This includes, but is not limited to, the uploading or creation of computer viruses, the willful damage of computer hardware, whether connected to the network or not, the deletion of data from its place of storage. Staff must contact the Network Support staff if they witness any activity of this nature.

6.9 Health and Safety
Health & Safety guidelines will be distributed alongside this document and the portable device. The AAT will take no responsibility for the implications resulting from not adhering to the suggested posture and handling of equipment in relation to, but not limited to repetitive strain injury (RSI) or eye strain.

Any staff experiencing discomfort when using the technology for a long period of time, should speak to the HR Manager within their school to request a workstation assessment.

6.10 Return of Equipment

Staff must take reasonable steps to ensure that the items can be returned to their school in a fit state for a subsequent user. Staff will be required to return all items on or before their last day at the school. In the event of failure to return all items of equipment on the last day of school, or as close to this as practicable, the school reserves the right to withhold an amount commensurate with the loss to the school from final salary payments. This also applies to accessories that have been issued (e.g. charging cables, cases) as well as the laptop and iPad hardware itself.

6.11 Device Loan Agreement

Staff who have a device on loan from the school will be required to sign and follow the AAT Staff Device Loan Agreement (*see **Appendix** H*) upon receiving the loaned device. This agreement outlines the responsibilities, agreement and guidelines that are required to be followed when in possession of a school owned and loaned device.

6.12 Printing, Copying and Transmission of Data

- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents emailed, copied, scanned, shared or printed. This is particularly important when shared copiers (multi-function print, fax, scan and copiers) are used.
- Staff should ensure that the entire document has been copied or printed and check that the copier has not run out of paper. This is particularly important when copying or printing large documents.
- Staff should not leave the printer unattended when using it, as another person may pick up the printing by mistake.
- When sending data, the most secure method of transmission must be selected, especially where information is particularly sensitive or confidential. All staff should consider the risk of harm or distress that could be caused to the relevant data subject if the information was lost or sent to another person, then look at the most appropriate way of sending the information to the recipient.
- Send only the minimum amount of personal or sensitive information, by whichever method is chosen.

Sending information by email:

- Carefully check the recipient's email address before pressing send – this is particularly important where the 'to' field autocompletes.
- If personal or sensitive information is regularly sent via email, consider disabling the auto complete function and regularly empty the autocomplete list.
- Take care when replying 'to all' – do they really all need to receive the information being sent.
- If emailing sensitive information, password protect any attachments. Use a separate email or different method to communicate the password e.g. telephone call.
- When sending sensitive files, the use of secure file transfer systems is mandatory, such as Schoolsfx or HertsFX.

Sending information by post:

- Check that the address is correct.
- Ensure only the relevant information is in the envelope and that someone else's letter has not been included in error.
- Consider using tracking, e.g. recorded delivery or a courier if appropriate.

7. REPORTING & RESPONDING

Where a learner misuses the Trust's ICT systems or internet, the school will follow the procedures set out in their behaviour and/or safeguarding policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the Trust's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

AAT schools will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

If a member of staff becomes aware of pupils sharing nudes or semi nudes they should follow the Government guidance, Sharing nudes and semi-nudes: how to respond to an incident and report it immediately to a DSL. The DSL should then follow the Government guidance, Sharing nudes and semi-nudes: advice for education settings working with children and young people. DSLs are responsible for ensuring that all staff are aware of the guidelines and how to respond to an incident of pupils sharing nudes or semi nudes.

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

- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with trust and school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- all members of the school community will be made aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Lead, Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.
- if there is any suspicion that the incident involves any illegal activity or the potential for serious harm (*see flowchart and user actions chart in the* ***Appendix I***), the incident must be escalated through the agreed school safeguarding procedures.

8. ONLINE SAFETY EDUCATION

8.1 Curriculum

Online safety is fully embedded within our curriculum. The school provides a comprehensive age appropriate curriculum for online safety which enables children and young people to become informed, safe and responsible. This includes teaching to prevent radicalisation, for which staff provide a narrative to counter extremism. The Personal Development/PSHE curriculum, Relationships and Health Curriculum are central in supporting the delivery of online safety education.

The curriculum is flexible and can respond to any immediate online safety issues and risks as they emerge.

It is necessary for children and young people to develop skills of critical awareness, digital resilience and good online citizenship to enable them to use internet, mobile and digital technologies safely and

responsibly. children and young people are taught to recognise the creative, collaborative, cultural, economic and educational opportunities provided by the internet, mobile and digital technologies.

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

- A planned online safety curriculum for all year groups matched against a nationally agreed framework and regularly taught in a variety of contexts.
- Lessons are matched to need; are age-related and build on prior learning
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
- Learner need and progress are addressed through effective planning and assessment
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; SRE; Literacy etc
- it incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- the programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- it is accepted that from time to time, for good educational reasons, learners may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need
- the online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.

8.2 Staff/volunteers

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

- a planned programme of formal online safety and data protection training will be made available to all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- the training will be an integral part of the school's annual safeguarding and data protection training for all staff
- all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements.
- the Online Safety Lead and Designated Safeguarding Lead will receive regular updates through attendance at external training events and safeguarding bulletins, and by reviewing guidance documents released by relevant organisations
- this Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days
- the Online Safety Lead will provide advice and training to individuals as required.

8.3 Governors and Trustees

Governors and Trustees should take part in online safety training/awareness sessions, with particular importance for those who are involved in online safety and safeguarding. A higher level of training will be made available to (at least) the Safeguarding Governors and Trustee.

8.4 Parents/Carers

The school works closely with families to help ensure that children can use internet, mobile and digital technologies safely and responsibly both at home and school. The support of parents/carers is essential to implement the online safety policy effectively and help keep children safe.

It is important that parents/carers understand the crucial role they play in this process. The school seeks to regularly consult and discuss online safety with parents/carers and seeks to promote a wide understanding of the benefits of new technologies and associated risks. The school provides regular updated online safety information through the school website, newsletters and by other means.

9. ACCEPTABLE USAGE

The AAT recognises that internet, mobile and digital technologies provide positive opportunities for children and young people to learn, socialise and play but they also need to understand the challenges and risks. The digital world is an amazing place, but with few rules. It is vast and fast moving and young people's future economic success may be partly dependent on their online skills and reputation. We are, therefore, committed to ensuring that all children and young people, staff, governors and Trustees will be supported to use internet, mobile and digital technologies safely. This is part of our safeguarding responsibility. Staff are aware that some children and young people may require additional support or teaching, including reminders, prompts and further explanation to reinforce their knowledge and understanding of online safety issues.

We are also committed to ensuring that all those who work with children and young people, including their parents/carers, are informed about the ever-changing risks so that they can take an active part in helping children and young people navigate the online world safely and confidently.

9.1 Scope

Acceptable usage applies to:

- children and young people
- parents/carers
- teaching and support staff
- school governors/trustees
- peripatetic teachers/coaches, supply teachers, student teachers
- visitors
- volunteers
- voluntary, statutory or community organisations using the school's facilities

The school also works with partners and other providers to ensure that children and young people who receive part of their education off site or who are on a school trip or residential are safe online.

The school provides online safety information for parents/carers, for example, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting their child/ren to behave appropriately and keep themselves safe online.

This policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community. It is linked to the following other school policies and documents: safeguarding, Keeping Children Safe in Education, GDPR, health and safety, home–school agreement, home learning, behaviour, anti-bullying and PSHCE/RSE, remote learning and any other relevant policies.

10. ACCEPTABLE USAGE PROCEDURE

The school seeks to ensure that internet, mobile and digital technologies are used effectively and safely, for their intended educational purpose, in ways that will not infringe legal requirements or create unnecessary risk.

The school expects everyone to use internet, mobile and digital technologies responsibly and strictly according to the conditions set out in this policy. This policy also includes expectations on appropriate

online behaviour and use of technology outside of school for children and young people, parents/carers, staff, governors and trustees and all other visitors to the school.

10.1 Use of email

Staff, governors and trustees should use a school email account or Governor Hub for all official school communication to ensure everyone is protected through the traceability of communication. Under no circumstances should staff contact children and young people, parents or conduct any school business using a personal email address. children and young people should use school approved accounts on the school system for educational purposes. Where required parent/carer permission will be obtained for the pupil account to exist. For advice on emailing, sharing personal or confidential information or the need to gain parent permission refer to the policy for GDPR. Emails created or received as part of any school role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.

Staff, governors and children and young people should not open emails or attachments from suspect sources and should report their receipt to the central AAT IT Team or their on-site school Network Support Team.

Users must not send emails which are offensive, embarrassing or upsetting to anyone (i.e. cyberbullying).

10.2 Visiting online sites and downloading

- Staff must preview sites, software and apps before their use in school or before recommending them to children and young people. Before using any online service that requires user accounts to be created or the sharing of any personal data, staff must consult with the central AAT IT Team or your on-site school Network Support Team. with details of the site/service and seek approval from a senior leader. The terms and conditions of the service should be read and adhered to, and parental/carer permission sought where required. If internet research is set for homework, specific sites will be suggested that have been checked by the teacher. All users must observe copyright of materials from electronic sources.

- Staff must only use pre-approved systems if creating blogs, wikis or other online content.

- When working with children and young people searching for images should be done through Google Safe Search (standard through the HICS service), Google Advanced Search or a similar application that provides greater safety than a standard search engine.

Users must not:

Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Indecent images of children actually or apparently under the age of 18 or images of child abuse (i.e. images of children, digital or cartoons, involved in sexual activity or posed to be sexually provocative)

- Indecent images of vulnerable people over the age of 18 (i.e. images of vulnerable people, digital or cartoons involved in sexual activity or posed to be sexually provocative)

- Adult material that breaches the Obscene Publications Act in the UK

- Promoting discrimination of any kind in relation to the protected characteristics: age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race or ethnicity, religion or belief, sex, sexual orientation

- Promoting hatred against any individual or group from the protected characteristics above
- Promoting illegal acts including physical or sexual abuse of children or adults, violence, bomb making, drug and alcohol abuse and software piracy
- Any material that may bring the school or any individual within it into disrepute e.g. promotion of violence, gambling, libel and disrespect

Users must not:

- Reveal or publicise confidential or proprietary information
- Intentionally interfere with the normal operation of the internet connection, including the propagation of computer viruses
- Transmit unsolicited commercial or advertising material either to other users, or to organisations connected to other networks except where permission has been given to the school
- Use the school's hardware and Wi-Fi facilities for running a private business
- Intimidate, threaten or cause harm to others
- Access or interfere in any way with other users' accounts
- Use software or hardware that has been prohibited by the school

All breaches of prohibited behaviours detailed above will be investigated, where appropriate, in liaison with the police.

The school recognises that in certain planned curricular activities, access to controversial and/or offensive online content may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned, risk assessed and recorded, and permission given by the member of staff responsible for Online Safety within the school.

10.3 Storage of Images

Photographs and videos provide valuable evidence of children and young people' achievement and progress in a variety of contexts and can be used to celebrate the work of the school. In line with GDPR they are used only with the written consent of parents/carers which is secured in the first instance on a child's entry to the school. Records are kept on file and consent can be changed by parents/carers at any time. (See **AAT GDPR Policy** for greater clarification).

Photographs and images of children and young people are only stored on the school's agreed secure networks which include some cloud-based services. Rights of access to stored images are restricted to approved staff as determined by the member of staff within the school who is responsible for online safety. Staff and children and young people may have temporary access to photographs taken during a class session, but these will be transferred/deleted promptly.

Parents/carers should note that there may be some children who are at risk and must not have their image put online and others who do not want their image online. For these reasons parents/carers must follow the school's Acceptable Use Agreement and refrain from taking or posting online photographs of any member of the school community, other than their own child/ren.

Staff and other professionals working with children and young people, must only use school equipment

to record images of children and young people whether on or off site. See also GDPR. Permission to use images of all staff who work at the school is sought on induction and a written record is located in the personnel file.

10.4 Use of mobile technologies
The school allows the use of mobile technologies as outlined in ***Appendix J***.

10.5 New technological devices
New personal technological devices may offer opportunities for teaching and learning. However, the school must consider educational benefits and carry out risk assessment before use in school is allowed. Parents/carers, children and young people and staff should not assume that new technological devices will be allowed in school and should check with IT/Network Support before they are brought into school.

11. STAFF TRAINING

Staff, governors and trustees are trained to fulfil their roles in online safety. The school audits the training needs of all school staff and provides regular training to improve their knowledge and expertise in the safe and appropriate use of internet, mobile and digital technologies. This training is recorded as part of safeguarding records.

New staff are provided with a copy of the online safety policy and must sign the school's Acceptable Use Agreement (*see* ***Appendix A***) as part of their induction and before having contact with children and young people.

Any organisation working with children and based on the school premises are also provided with a copy of the online safety policy and required to sign the Acceptable Use Agreement (*see* ***Appendix B***)

Peripatetic staff, student teachers and regular visitors are provided with a copy of the online safety policy and are required to sign the Acceptable Use Agreement (*see* ***Appendix B***).

Guidance is provided for occasional visitors, volunteers and parent/carer helpers (*see* ***Appendix C***).

12. WORKING IN PARTNERSHIP WITH PARENTS/CARERS

The school works closely with families to help ensure that children can use internet, mobile and digital technologies safely and responsibly both at home and school. The support of parents/carers is essential to implement the online safety policy effectively and help keep children safe.

It is important that parents/carers understand the crucial role they play in this process. The school seeks to regularly consult and discuss online safety with parents/carers and seeks to promote a wide understanding of the benefits of new technologies and associated risks. The school provides regular updated online safety information through the school website, newsletters and by other means.

Parents/carers are asked on an annual basis to read, discuss and co-sign with each child the Acceptable Use Agreement. A summary of key parent/carer responsibilities will also be provided and is available in ***Appendix F***. The Acceptable Use Agreement explains the school's expectations and pupil and parent/carer responsibilities.

13. MONITORING AND REPORTING

The school recognises the need to record online safety incidents and to monitor and review policies and procedures regularly in order to ensure they are effective and that the risks to children and young people and staff are minimised. AAT uses NetSupport classroom.cloud as its monitoring and classroom management solution across the majority of schools in the Trust, with the exception of Verulam School

using Smoothwall Monitor. All schools within the trust are with HFL for their broadband service which provides the filtering solution through RM Safety Net. All staff, students and school owned devices are required to have both filtering and monitoring in place. AAT/schools reserve the right to monitor all activity on AAT/school owned devices and systems for both safeguarding and wellbeing purposes. Students who are part of the BYOD scheme are required to have monitoring on their devices following the latest guidance and requirements from 'Keeping Children Safe In Education' and the related 'DfE Technical Standards'.

All breaches of this policy must be reported to the DSL. All staff have the individual responsibility to ensure that incidents have been correctly recorded, acted upon and reported. DSLs are responsible for ensuring records are kept which will allow for patterns of concerning behaviour to be identified.

The school supports children and young people and staff who have been affected by a policy breach. Where there is inappropriate or illegal use of internet, mobile and digital technologies, this will be dealt with under the school's behaviour and disciplinary policies as appropriate. Breaches may also lead to criminal or civil proceedings.

AAT schools have the right to examine any data or files on an electronic device where there is a good reason to do so. Staff members must have regard to the following guidance issued by the Secretary of State when determining what is a "good reason" for examining or erasing the contents of an electronic device: In determining a 'good reason' to examine or erase the data or files the staff member should reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules.

Governors and trustees receive termly summary data on recorded online safety incidents for monitoring purposes. In addition, trustees ensure they have sufficient, quality information to enable them to make a judgement about the fitness for purpose of this policy on an annual basis.

14. APPENDICES OF THE ONLINE SAFETY POLICY

A. Online Safety Acceptable Use Agreement - Staff, Governors and student teachers (on placement or on staff)
B. Online Safety Acceptable Use Agreement - Peripatetic teachers/coaches, supply teachers
C. Requirements for visitors, volunteers and parent/carer helpers working in the school (working directly with children or otherwise)
D. Online Safety Acceptable Use Agreement Primary children and young people
E. Online Safety Acceptable Use Agreements Secondary children and young people
F. Online safety policy guide - Summary of key parent/carer responsibilities
G. Guidance for staff on preventing and responding to negative comments on social media
H. Staff Device Loan Agreement
I. Online Safety incident Flowchart
J. Use of Mobile Technologies

APPENDIX A - Online Safety Acceptable Use Agreement - Staff, Governors, Trustees and student teachers (on placement or on staff)

You must read this agreement in conjunction with the IT Acceptable Use & Online Safety policy and the GDPR policy. Once you have read these, you must sign and submit this agreement and it will be kept on record in the school. You should retain your own copy for reference. This forms part of your professional and safeguarding responsibilities.

Internet, mobile and digital technologies are part of our daily working life and this agreement is designed to ensure that all staff, governors and trustees are aware of their responsibilities in relation to their use. All staff, student teachers, governors and trustees are expected to adhere to this agreement and to the IT Acceptable Use & Online Safety policy. Any concerns or clarification should be discussed with the member of staff within the school who is responsible for online safety. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.

Internet Access

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to the member of staff responsible for online safety and/or DSL and an incident report completed.

Online conduct

I will ensure that my online activity, both in and outside school, will not bring the Trust, school, my professional reputation, or that of others, into disrepute.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see policy).

I will report any accidental access to or receipt of inappropriate materials or filtering breach on the school's Online Safety log.

I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager, headteacher and others as required.

I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to children and young people and/or parents/carers where my school role is my only connection to them.

Social networking

I understand and will follow the guidance outlined in the AAT Social Media Policy.

Passwords

I understand that there is no occasion when a password should be shared with a pupil or anyone who is not a staff member.

Data protection

I will follow requirements for data protection as outlined in GDPR policy. These include:

- Photographs must be kept securely and used appropriately, whether in school, taken off the school premises or accessed remotely
- Personal data can only be taken out of school or accessed remotely when authorised by the headteacher or governing board
- Personal or sensitive data taken off site must be encrypted

Images and videos

I will follow the published school guidance on taking images, videos and sound recordings of school events or activities on any device.

I will follow the published school guidance on uploading images or videos of staff, children and young people or parents/carers onto school approved sites where specific permission has been granted.

Use of email

I will use my school email address or governor hub for all school business. All such correspondence must be kept professional and is open to Subject Access Requests under the Freedom of Information Act. I will not use my school email addresses or governor hub for personal matters or non-school business.

Use of personal devices

I understand I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices. I understand that the use of personal devices in school is at the discretion of the headteacher.

I will always act responsibly, safely and respectfully in line with current school acceptable use agreements and safe working practices.

Additional hardware/software

I will not install any hardware or software on school equipment without permission of Network Support (For schools with no Network Support staff onsite please contact IT contact within the home school).

Promoting online safety

I understand that online safety is the responsibility of all staff, governors and trustees and I will promote positive online safety messages at all times including when setting homework or providing pastoral support.

I understand that it is my duty to support a whole school safeguarding approach and will report any inappropriate or concerning behaviour (of other staff, governors, trustees, visitors, children and young people or parents/carers) to the DSL.

Classroom management of internet access

When lesson planning, I will pre-check for appropriateness of all internet sites used in the classroom. This will include the acceptability of other material visible, however briefly, on the site. I will not free-surf the internet

in front of children and young people. When lesson planning, I will also check the appropriateness of any suggested sites suggested for home learning.

If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use with the DSL.

User signature

I agree to follow this Acceptable Use Agreement and to support online safety throughout the school. I understand this forms part of the terms and conditions set out in my contract of employment (staff members only) and/or my responsibilities as a governor/trustee.

Signature …….…….…… Date ……
Full Name …….…… (printed)
Job title ……

APPENDIX B - Online Safety Acceptable Use Agreement - Peripatetic teachers/coaches, supply teachers

School name:<<enter school name>>

Member of Staff Responsible for Online Safety:<<enter name>>

Designated Safeguarding Lead (DSL):<<enter name>>

This agreement forms part of your professional and safeguarding responsibility in the school. You must read and sign this agreement. This will be kept on record and you should retain your own copy for reference.

Internet, mobile and digital technologies are part of our daily working life and this agreement is designed to ensure that all staff and governors and trustees are aware of their responsibilities in relation to their use. You are expected to adhere to this agreement. Any concerns or clarification should be discussed with the DSL. Breaches will be investigated, recorded and, where appropriate, disciplinary procedures will apply and police involvement will be sought.

The Trust's IT Acceptable Use & Online Safety policy will provide further detailed information as required.

Internet Access

I will not access or attempt to access any sites that contain any of the following: child abuse; pornography; discrimination of any kind; promotion of prejudice against any group; promotion of illegal acts; any other information which may be illegal or offensive. Inadvertent access on school equipment must be treated as an online safety incident, reported to the member of staff responsible for online safety and/or DSL and an incident report completed.

Online conduct

I will ensure that my online activity, both in and outside school, will not bring the Trust, school, my professional reputation, or that of others, into disrepute.

I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. Exceptionally, use of controversial material as part of the curriculum should be planned and approved on every occasion (see policy).

I will report any accidental access to or receipt of inappropriate materials or filtering breach to the DSL.

I understand that all my use of the internet and other related technologies can be traced and monitored and, should it be required, must be made available to my line manager, headteacher and others as required.

I will not give out my personal contact and online account information such as phone numbers, email address, and social media account details to children and young people and/or parents/carers.

Should I need to share my professional details, such as mobile phone number or email address, with parent/carers, this must be agreed in advance as an acceptable approach with the DSL.

Social networking

I understand and will follow the guidance outlined in the AAT Social Media Policy.

Passwords

I must clarify what access I may have to the internet and/or school systems. If I have access of any kind, I understand that there is no occasion when a password should be shared with a pupil or anyone who is not a staff member.

Data protection

I will follow all requirements for data protection explained to me by the school. These include:

- I must consult with the school before making any recordings, photographs and videos. Once agreed, these must be made on a school device.

- I understand that there are strict controls and requirements regarding the collection and use of personal data. I will follow all requirements regarding GDPR.

Images and videos

I will only upload images or videos of staff, children and young people or parents/carers onto school approved sites where specific permission has been granted.

I will not take images, sound recordings or videos of tuition or wider school activities on any personal device. School devices can be used for this purpose or, in the case of 1:1 tuition, pupil's or parent/carer devices can be used, with parent/carer agreement.

Internet, mobile and digital technologies provide helpful recording functions but these cannot be made on a teacher's personal device. Recordings can be made with the child's and parent/carer's agreement on a school device, an organisational device approved by the headteacher/DSL, or a young person's or parent/carer's own device.

Use of Email

I will only use my professional email address for all school business. All such correspondence should be kept professional and is open to Subject Access Requests under the Freedom of Information Act. I will not use my professional email addresses for personal matters.

Use of personal devices

I understand that when working in the school I should at no time put myself in a position where a safeguarding allegation can be made against me as a result of my use of personal devices. I understand that the use of personal devices in school is at the discretion of the headteacher.

I will always act responsibly, safely and respectfully in line with current school acceptable use agreements and safe working practices.

Additional hardware/software

I will not install any hardware or software on school equipment without permission of Network Support (or the contact stated in the AAT IT Acceptable Use policy where no onsite Network Support).

Promoting online safety

I understand that online safety is part of my responsibility and I will promote positive online safety messages at all times, including when setting homework, rehearsal or skill practice or when providing pastoral support.

I understand that it is my duty to support a whole school safeguarding approach and will report any behaviour (of staff, governors, visitors, children and young people or parents/carers) which I believe may be inappropriate or concerning in any way to the DSL.

Classroom management of internet access

I will pre-check for appropriateness all internet sites used in the classroom or during a tutoring session; this will include the acceptability of other material visible, however briefly, on the site. I will not free-surf the internet in front of children and young people.

If I am using the internet to teach about controversial issues I will secure, on every occasion, approval in advance for the material I plan to use with the DSL.

User Signature

I agree to follow this Acceptable Use Agreement and to support online safety in my work in the school. I understand this forms part of my company/educational setting/organisation's contract with the school.

Signature ……..……..……..……..… Date ……..……
Full Name ……..…… (Please use block capitals)
Job Title/Role ……..……..……

APPENDIX C - Requirements for visitors, volunteers and parent/carer helpers
(Working directly with children or otherwise)

School name:<<enter school name>>

Member of Staff Responsible for Online Safety:<<enter name>>

Designated Safeguarding Lead (DSL):<<enter name>>

This document is designed to ensure that you are aware of your responsibilities when using any form of IT in the school and other aspects of safeguarding in connection with online safety.

Please raise **any** safeguarding concerns arising from your visit immediately with the headteacher and/or DSL.

- I understand I may only use my personal mobile phone(s) and other devices with camera functions in designated areas. When not in a designated area, phones must be switched off and out of sight. Any exception must be pre-arranged.

- I will not take images, sound recording or videos of school events or activities, on or off site, on any device. Any possible exception must be pre-arranged.

- I will not give out my personal details such as mobile phone number, email address, and social media account details to children and young people. Where appropriate I may share my professional contact details with parents/carers provided the DSL or headteacher is informed before I leave the school.

- I understand my visit to the school may give me access to privileged information about children and young people, staff, school systems and plans. Such information should never be shared on line, including on social media sites.

- I understand I should not use school equipment to access the internet without prior approval from my contact in the school or the headteacher.

- If working in the classroom, I will pre-check for appropriateness all internet sites I intend to use including checking the acceptability of other material visible on the site. I will not free-surf the internet in front of children and young people. If I am in any doubt about the appropriateness of the content I plan to use I will check with my contact in the school.

Signature ……..……..……..…… Date ……..……
Full Name ……..…… (Please use block capitals)
Job Title/Role ……..……..……

APPENDIX D - Online Safety Acceptable Use Agreement Primary children and young people

My Online Safety Rules

- I will only use school IT equipment for activities agreed by school staff.
- I will not use my personal email address or other personal accounts in school
- I will not sign up for any online service on school devices unless this is an agreed part of a school project approved by my teacher and agreed by my parent/carer.
- I will only open email attachments if it has been approved by a member of school staff in school or a parent/carer out of school.
- In school I will only open or delete my files when told by a member of staff.
- I will not tell anyone other than my parents/carers my passwords. I will not use other people's usernames or passwords to pretend to be them online.
- I will make sure that all online contact I make is responsible, polite and sensible. I will be kind and respectful at all times.
- If I come across anything upsetting, unpleasant or nasty, or anything that makes me feel unsafe, I will tell my teacher or my parent/carer immediately.
- If someone says, asks or posts about me anything upsetting, unpleasant or nasty, or anything that makes me feel unsafe, I will not reply. I will tell my teacher or my parent/carer immediately.
- I will not give out my own or other people's personal information, including: name, phone number, home address, interests, schools or clubs. I will tell my teacher or parent/carer if anyone asks me online for personal information.
- Uploading or sending my image (photographs, videos, live streaming) online puts me at risk. I will always seek permission from my teacher or parent/carer if I wish to do this. I will not take, share or upload any image of anyone else without their permission and also, if they are a child, without their parent's/carer's permission.
- Even if I have permission, I will not upload any images, videos, sounds or words that **could** upset, now or in the future, any member of the school community, as this is cyberbullying.
- I understand that some people on the internet are not who they say they are and some people are not safe to be in contact with. I will not arrange to meet someone I only know on the internet. If someone asks to meet me, I will not reply to them and I will tell a teacher or a parent/carer immediately.
- I understand that everything I do or receive online can be traced now and in the future. I know it is important to build a good online reputation.
- I understand that some personal devices are allowed in school and some are not, and I will follow the rules. I will not assume that new devices can be brought into school without getting permission.
- I understand my behaviour in the virtual classroom should mirror that in the physical classroom
- I will not lie about my age in order to access games, apps or social networks that are for older people as this will put me at risk.
- I understand that these rules are designed to keep me safe now and in the future. If I break the rules my teachers will look into it and may need to take action.

Dear Parent/Carer,

The internet, email, mobile technologies and online resources have become an important part of learning and life. We want all children to be safe and responsible when using any IT. It is essential that children are aware of online risk, know how to stay safe and know where to go to report problems or to get help.

Please read through these online safety rules with your child/ren and talk with them to ensure they understand their importance and what it means for them (and for you). When you have done this, you both need to sign this agreement to say that you agree to follow the rules. Any concerns or explanation can be discussed with your child/ren's teacher.

Please return the signed sections of this form which will be kept on record at the school.

Pupil agreement

Pupil name……..…

This agreement is to keep me safe. I have discussed this agreement with my parents/carers and understand the commitment I have made and my responsibilities.

Pupil signature……..

Parent(s)/Carer(s) agreement

Parent(s)/Carer(s) name(s)…….

I/we have discussed this agreement, which highlights the associated risks when accessing the internet, mobile and digital technologies, with our child/ren. I/we agree to support them in following the terms of this agreement.

I/we also agree not to share school related information or images online or post material that may bring the school or any individual within it into disrepute.
(Rather than posting negative material online, any parent, distressed or concerned about an aspect of school should make immediate contact with a member of staff. Negative postings about the school would impact on the reputation of the whole school community. Parents are encouraged to report breaches so that we can protect the reputation of the school, staff, children and young people and parents).

I/we also agree only to use personal mobile phones and devices in designated areas of the school unless otherwise informed, e.g. for specific events and activities. I/we understand that under no circumstance should images be taken at any time on school premises of anyone other than our own child/ren, unless there is a pre-specified agreement. I/we understand that when on school premises, but not in a designated area where phones can be used, they must be switched off and out of sight.

Parent(s)/Carer(s) agreement

Parent(s)/Carer(s) name(s)…….

Parent/carer signature……. Date ……

APPENDIX E - **Online Safety Acceptable Use Agreement Secondary children and young people**

- I will only use school IT equipment for school purposes.
- I will not download or install software on school IT equipment.
- I will only log on to the school network, other school systems and resources using my own school username and password.
- I will not reveal my passwords to anyone other than a parent/carer.
- I will not use my personal email address or other personal accounts on school IT equipment.
- I will make sure that all my electronic communications are responsible and sensible.
- I understand my behaviour in the virtual classroom should mirror that in the physical classroom.
- I understand that everything I search for, access, post or receive online can be traced now and in the future. My activity can be monitored and logged and if necessary shared with teachers, parents/carers and the police if necessary. I know it is essential that I build a good online reputation.
- I will not browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material, I will report it immediately to a member of staff if I am in school, or parent/carer if I am not in school.
- I will not give out my own or others' personal information, including: name, phone number, home address, interests, schools or clubs or any personal image. I will immediately report any request for personal information, to a member of staff if I am in school or parent/carer if I am not in school.
- I should never post photographs, videos or livestream without the permission of all parties involved.
- I will not upload any images, videos, sounds or words that **could** upset, now or in the future, any member of the school community, as this is cyberbullying.
- I will be respectful to everyone online; I will treat everyone the way that I want to be treated. I will ensure that all my online activity, both in and outside school, will not cause distress to anyone in the school community or bring the school into disrepute.
- I will not respond to hurtful behaviour online but will report it. I have the right to block and will say no to any inappropriate or upsetting request.
- I will respect the privacy and ownership of others' work on-line and will adhere to copyright at all times.
- I will not attempt to bypass the internet filtering system in school.
- I will not assume that new technologies can be brought into school and will check with staff before bringing in any device.
- I will not lie about my age in order to sign up for age inappropriate games, apps or social networks.
- I understand that not everything I see or hear online is true, accurate or genuine. I also know that some people on the internet are not who they say they are and may have ulterior motives for assuming another identity that will put me at risk. I will gain permission from parents/carers before arranging to meet someone I only know on the internet.
- I understand that these rules are designed to keep me safe now and in the future. If I break the rules, teachers will investigate, I may be disciplined and my parents/carers may be contacted. If I break the law the police may be informed.

Bring Your Own Device (Delete section if no BYOD)

- I will bring my device to school with me each day. I am aware that I will receive consequences in line with the consequence system should I not have the correct equipment for school (year 7-11). Temporary loan devices can be borrowed for a day should I not have a device with me. If I borrow a device and do not return it at the end of the school day, then I will be sanctioned.
- If I bring a mobile phone to school, I know that this must be switched off and cannot be used whilst I am on campus throughout the school day (year 7-11). I will not be able to use my phone as a device for learning within my lessons.
- If I am participating in the school loan scheme, I understand that all tablets or laptops remain the property of <<enter school name>> and are on loan to me while I am on roll at school. I understand that loan devices must be returned on request.
- My own portable device will only be used for learning purposes during school time. Sanctions will apply for inappropriate use of my device during lessons.
- My teacher has full discretion to ask me to put my device away in any lesson or at any time.
- When I bring my own device to school, I am fully responsible for keeping it safe. My device will be fully charged before coming to school. I will store my device safely when it is not being used (e.g. in my locker.)
- I will ensure that my device has a passcode or other locking system to ensure that my personal information remains safe. I will not use another person's device without their permission.
- With my own device, I will only connect to the school WiFi network to use the Internet. I will not enable 3G/4G during school time for my own protection and to protect the privacy of staff and students.
- I will not take or post photographs, videos or livestream without the permission of all parties involved. I will not post any images to social media taken during school time without permission. I will delete any image or video if I am asked to do so by a member of staff. I understand that teachers have the right under law to search my device for material that may be harmful.
- Whilst I am allowed to install my own software and media on my own device, I understand that space must be given to learning applications and I may be asked to delete other content to make space for learning tools.
- My own device must not contain illegal software, must not be 'Jailbroken' and must have regular official updates applied from the manufacturer in order to keep secure.
- I understand that my device will be filtered and monitored by the school.
- My device is required to have AAT/School monitoring software on for safeguarding and wellbeing purposes.
- I will ensure that the schools monitoring solution is enabled on my device and I will not remove, tamper or disable this.
- If available, I will ensure my device has adequate antivirus and spyware protection and that it is kept up to date to prevent damage to other devices on the school network.

I understand that these rules are designed to keep me safe now and in the future.

I understand that my network and Internet access may be taken away if I fail to abide by these rules. In accordance with school policy, devices may be confiscated for a limited time period.

I understand that I am subject to sanctions laid down in the rewards and consequences policy and other applicable school policies. If I break the law the police may be informed.

By accepting your place at <<enter school name>>, you agree and consent to abide by all the instructions and requirements detailed in this acceptable use policy.

APPENDIX F - Online safety policy guide - Summary of key parent/carer responsibilities

The school provides online safety information for parents/carers, through the website, in newsletters and at events. It is important that parents/carers understand their key role in supporting children to behave appropriately and keep themselves safe online.

The online safety policy, supported by its acceptable use agreements, is intended to protect the interests and safety of the whole school community.

- Parents/carers are required to support their child in understanding and signing the Online Safety Acceptable Use Agreement for children and young people.

- Parents/carers may only use personal mobile phones and devices in designated areas of the school unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises that include anyone other than their own child, unless there is a pre-specified agreement with individuals and parents/carers. When a parent/carer is on school premises but not in a designated area, their phone/s must be switched off and out of sight.

- Parents/carers should not assume that children and young people can bring technological devices to school and should always check the school policy.

- All cyberbullying incidents affecting children in the school should be reported immediately. (If the incident involves an indecent image of a child the report must also be made immediately to the police for your own protection.) The school will investigate and respond to all reported cyberbullying incidents, liaising with others where appropriate. No reply should ever be sent to the sender/poster of cyberbullying content. If applicable, block the sender and report abuse to the site. Evidence should be retained and shown in school and/or to the police. Evidence should not be forwarded.

- The school may choose to set up social media sites, blogs or have some other online presence in its own name. Parents/carers, however, do not have the right to set up any site, page, chat group or any other online presence that uses the school name or logo in any form.

- Any parent/carer, distressed or concerned about an aspect of school should make immediate contact with a member of staff rather than posting their concerns online. Parents/carers should not share school related information or images online or post material that may bring the school or any individual within it into disrepute. Negative postings about the school would impact on the reputation of the whole school community. Parents/carers are encouraged to report breaches so that we can protect the reputation of the school, staff, children and young people and parents/carers.

Please see the full IT Acceptable Use & Online safety policy in the policies section on the Trust website.

APPENDIX G - Guidance for staff on preventing and responding to negative comments on social media

The school should make it clear which, if any, social media platforms are used to communicate with parents/carers. If used correctly, parents can use a school's social media site as a source of reliable information. The IT Acceptable Use & Online safety policy, see especially Appendix VI (Online safety policy guide - Summary of key parent/carer responsibilities), clarifies that no other social media platforms should be set up using the school's name or logo.

The school should regularly reinforce with all parties that discussion of school issues on social media platforms, either positive or negative, should not take place as this could bring the school into disrepute and affect families and children. Parents should be encouraged to be good online role models and not post statements written in anger or frustration. Identified routes to raise concerns directly with the school should be used.

If negative comments are posted:

- Collect the facts

As soon as you become aware of adverse comments relating to the school you need to establish what is being said. It is essential that if you have access to the postings they are secured and retained together with any other evidence. Do not become engaged in responding directly.

If the allegations against a member of staff or a pupil are of a serious nature, these will need to be formally investigated. This may involve the police and the headteacher will need to follow the school's safeguarding procedures.

If there is a risk of serious damage to the school reputation or the reputation of individual members of staff, professional legal advice should be sought.

Adverse comments of any kind are highly demotivating and cause stress and anxiety. It is important that the senior staff reassure and support all staff and/or other affected members of the school community.

Addressing negative comments and complaints

Contact the complainants and invite them to a meeting. In the meeting, make sure you have any evidence available.

The meeting must:

- Draw attention to the seriousness and impact of the actions/postings;
- Ask for the offending remarks to be removed;
- Explore the complainant's grievance;
- Agree next steps;
- Clarify the correct complaints procedures.

If the meeting does not resolve the issue, the parents must be informed that the school will need to take the matter further. This may include:

- Reporting the matter to the social network site if it breaches their rules or breaks the law;
- Reporting the matter to the police if it breaks the law, e.g. if the comments are threatening, abusive, malicious, sexist, of a sexual nature, constitute a hate crime or are libellous they may well break the law. Online harassment and stalking is also a crime.

If inappropriate postings continue or the original material is not removed, a second meeting is advisable to reiterate the seriousness of the matter.

APPENDIX H - Staff Device Loan Agreement

	AAT Device Loan Agreement	
Alban Academies Trust	**Last reviewed:** March 2023	**Next Review:** March 2025

1 RESPONSIBILITIES

- I will follow the guidance of the AAT IT Acceptable Use & Online Safety (Including Online Safety Acceptable Use Agreements) Policy
- I will follow the guidelines listed below for proper care of the laptop.
- I will use the computer for school or professional development purposes only.
- I will not attempt to install any software on the computer unless it has been approved by a member of the IT/Network Support Team.
- Requests for software modification or installation should be made 7 days in advance of when they are needed to allow IT sufficient time to review, deploy and ensure systems compatibility and capabilities beforehand.
- I will not write on, place labels or stickers on the laptop.
- I will not disable, uninstall or tamper with the virus protection software that is provided with the device.
- I will ensure any documents I create are stored on Google Drive or local server drives and not the device itself.
- I will bring the laptop into school and log in to the network on a regular basis at a minimum, to ensure that antivirus and other updates that are pushed out through the network are current and kept up to date.
- I will report any problems or issues I encounter while using the laptop to the IT/Network Support Team immediately either in person or through the help desk.
- I understand that the IT/Network Support Team will reimage the device at any point where it becomes unusable, unstable or suspected of security breaches at any time. In the event of this occurrence, a loan device will temporarily be issued until the matter is resolved.
- I understand that reimaging, repairs or alterations on the device may result in the loss of all data stored locally on the laptop.
- Any modifications I make in the computer's settings will be for usability or accessibility purposes only.
- Laptops will be reassigned as deemed appropriate by the administration.

2 DEVICE GUIDELINES

- The laptop is not to be loaned to anyone.
- Other individuals, including children, should not be allowed to play on the computer.
- Appropriate care is to be always provided to the device, including but not limited to:
    a. Give care appropriate for any electrical device.
    b. Use a surge protector or unplug the laptop during electrical storms.
    c. Keep food and drink away from the computer.
    d. Do not leave the laptop exposed to direct sunlight or extreme cold.
    e. Position the laptop on a safe surface so it does not drop or fall.
    f. Do not attempt to repair a damaged or malfunctioning laptop.
    g. Do not attempt to upgrade the computer or software.
- Appropriate security is to be always provided for the device, including but not limited to:
    a. Secure your laptop in a safe place at the end of the day.
    b. Do not leave the laptop in an unlocked car.

c. Do not leave/store the laptop in a car overnight or when not in transit.
d. Do not leave the power supply behind when moving the laptop.

3 AGREEMENT

- I understand that all laptop computers, equipment, and/or accessories that AAT has provided to me, are the property of Alban Academies Trust.
- I agree to the terms outlined in the AAT IT Acceptable Use & Online Safety (Including Online Safety Acceptable Use Agreements) Policy.
- I understand that I will report any damage, loss, or theft of any devices, equipment and/or accessories on loan to me to the IT/Network Support Team as soon as possible.
- I understand that I will not be held responsible for computer problems as a result of regular school-related and acceptable use.
- I understand that I am personally responsible for any damage, theft, or loss of devices on loan to me and/or related equipment and accessories due to negligence. In the event of this occurring, you are responsible for the total value of costs to replace or repair the device, accessories or related equipment.
- I understand that a violation of the Device Loan Agreement and/or the AAT IT Acceptable Use & Online Safety (Including Online Safety Acceptable Use Agreements) Policy, will result in the restriction and/or termination of my use of the AAT laptop, computers, equipment, and/or accessories as a direct result.
- I understand that I am under obligation to return all devices listed below in the agreement including chargers and related peripherals, before or on my final contracted day with the school.

Device/Item Type	Make	Model	Serial Number	Condition
Details of Condition (Scuffs, Scratches, Dents, Markings etc) and other details: ▪ ▪ ▪ ▪				

Name (Printed): _____

Signature: _____

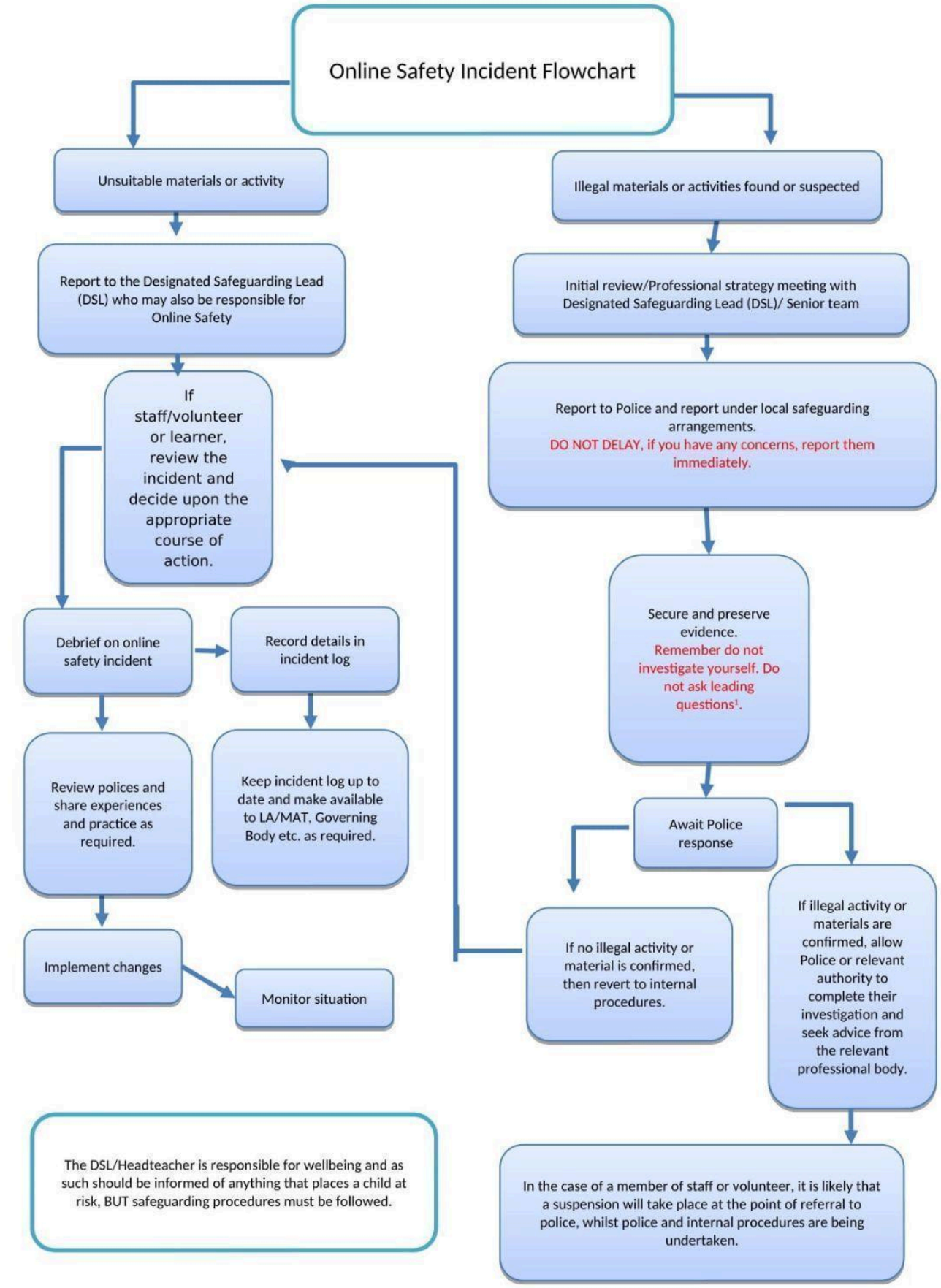
Date: _____

Advice for Laptop Users

You are responsible for your laptop. **Never** leave your laptop unattended in an unlocked room. Your laptop should at all times be either in your presence or locked away.

- You will usually receive with your laptop, a carry case, an iPad and the respective chargers. Please ensure to name these items, since they tend to go missing. Lost peripherals may only be replaced at a cost to your department.
- Be careful not to bump or drop your computer, do not carry items with it that could harm it and do not put any objects on top of it. The case, although strong, is not made to support extra weight.
- Take care when handling and storing external cables. They can be damaged very easily. Please do not leave power cables attached to the laptop when storing or transporting. Wrap and store loosely in your bag.
- When transporting your computer, always turn it off and put it in a carrying case, other than between lessons.
- Avoid subjecting the laptop to extreme temperature changes. Components can become very brittle and easy to break in cold temperatures and can melt or warp in high temperatures. As a general rule, your computer is safest at temperatures that are comfortable for you. Avoid storing your laptop on a radiator.
- Keep all liquids away from your laptop. Almost any liquid spilt on the computer will result in it being completely unusable.
- Keep your laptop away from magnetic fields. Magnetic fields can erase data on hard drives.
- You should make yourself aware of the Health and Safety advice concerning the use of computers (such as seating, posture, ergonomics, ambient lighting and taking breaks)
- Anti-virus software will be installed on your laptop, but you are under a direct obligation to ensure that updates are installed. Your laptop will be configured to auto-update its anti-virus software whenever you connect to the internet, either at home or at school, please ensure you do so at least once per week. If you suspect your computer is infected with a virus please report it to network support as soon as possible.
- Staff must not use or install unlicensed, malicious or gaming software.
- You must not create documents or files for which storage would contravene the Data Protection Act.
- Any material on the laptop must be in accordance with the law.
- Staff must notify Network Support of any additional applications needing to be installed on the laptop. The software must be legal (including demo or trial) and must be relevant for the position they hold.
- You should ensure that you take regular backup copies of your documents and other files that you have created. You may do this by transferring files to your Google Drive or an external hard drive.
- Be careful when working on a document or file at home that you have copied from another computer since they may be infected with viruses.
- If your laptop is stolen or lost, staff must immediately advise Network Support. This will ensure that recovery procedures can be activated as soon as is practicable.

APPENDIX I - Online Safety incident Flowchart



Other Incidents

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

- Concerns around pupil safeguarding must result in an immediate call to LADO : 01872 326536/324954 Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- 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)
- Once this has been completed and fully investigated it will needed to be judged whether this concern has substance or not. A conversation with LADO will help make a final decision regarding action to be taken. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority/School Group or national/local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the Police/LADO immediately. Other instances to report to the police would include:
    - incidents of ‘grooming’ behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act or criminally racist material or promotion of terrorism or extremism
    - offences under the Computer Misuse Act
    - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

APPENDIX J - Use Of Mobile Technologies

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 learning platform and other cloud-based services such as email and data storage.

All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational.

The school allows the following use of mobile technologies:

	School Devices			**Personal Devices**			
	School Owned And Allocated To A Single User	**School Owned For Use By Multiple Users**	**Authorised Device[3]**	**Pupil/Student Owned**		**Staff (Including Temporary And Peripatetic) Owned**	**Visitor Owned**
				Phone	**Tablet**		
Allowed In School	Yes	Yes	Yes	Yes	If BYOD in place	Yes	Yes
Needs To Remain Turned Off During School Day	No	No	No	Yes	If BYOD in place	No	No
Full Network Access	Yes	Yes	Yes	No	No	No	No
Internet Only	n/a	n/a	n/a	No	Yes	Yes	Yes

The school has provided technical solutions for the safe use of mobile technology for school devices/personal devices:

- All school devices are controlled through the use of Mobile Device Management (MDM) software
- Appropriate access control is applied to all mobile devices according to the requirements of the user (e.g. Internet only access, network access allowed, shared folder network access)
- The school has addressed broadband performance and capacity to ensure that core educational and administrative activities are not negatively affected by the increase in the number of connected devices
- For all mobile technologies, filtering will be applied to the internet connection and attempts to bypass this are not permitted
- Appropriate exit processes are implemented for devices no longer used at a school location or by an authorised user. These may include; revoking the link between MDM software and the device, removing proxy settings, ensuring no sensitive data is removed from the network, uninstalling school-licensed software etc.
- All school devices are subject to routine monitoring

[3] Authorised device – purchased by the pupil/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

- Pro-active monitoring has been implemented to monitor activity

When personal devices are permitted:

- All personal devices are restricted through the implementation of technical solutions that provide appropriate levels of network access (in some specific cases e.g. printing)
- Personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device in to the school lies with the user (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in school
- The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home)
- The school accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network or whilst resolving any connectivity issues
- Staff owned devices should not be used for personal purposes during teaching sessions, unless in exceptional circumstances

When using mobile technologies users are expected to act responsibly, safely and respectfully in line with current school acceptable use agreements and safe working practices.