



## IT – Acceptable Use & Online Safety (Including Online Safety Acceptable Use Agreements)

**Last reviewed:**  
May 2021

**Next Review:**  
May 2022

### 1 PRINCIPLES

The 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 pupils, 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 pupils 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
- Use of social media including school accounts on Facebook, Twitter and other social media applications

AAT Schools will all adopt the AAT Online Safety Policy (based on the model policy provided by Herts for Learning). Please see appendix A 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 Trustees are responsible for the approval of the AAT IT acceptable use and online safety policy and for reviewing the effectiveness of the policy.

Each AAT school will adopt the AAT Model Online Safety Policy (Appendix A) and adapt it to suit their school. This appendix will be reviewed in the same timeline as the overarching policy and any changes will be rolled out to all schools within the Trust.

The Governors at the member schools are responsible for the approval of the school's adapted version of the AAT model online safety policy (Appendix A). A member of the governing board has taken the role of Online Safety Governor, this role includes:

- regular meetings with the Online Safety Lead
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant Governor meetings

The Headteacher within an AAT school has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Lead. The Headteacher will ensure that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

The Online Safety Lead takes day to day responsibility for the online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents. They also:

- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- provides training and advice for staff
- liaises with the Local Authority/AAT/relevant bodies where relevant
- liaises with school technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- meets regularly with the Online Safety Governor to discuss current issues, review incident logs and filtering/change control logs
- attends relevant meetings of Governors
- reports regularly to the school Senior Leadership Team

The AAT Network Support staff including school Network Managers/Technical staff<sup>1</sup> 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 Online Safety Lead
- that monitoring software/systems are implemented and updated as agreed in school policies

---

<sup>1</sup> 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.

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

All other stakeholders (e.g. all other staff, pupils, parents, visitors, community users) are responsible for using the schools' digital technology systems in accordance with the school acceptable use agreements.

All breaches of this policy must be reported to the contacts contained in the schools' Online Safety Policies.

All breaches of this policy that may have put a child at risk must also be reported to the DSL within the schools, these are detailed in the schools' Online Safety Policy.

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 Trust's online safety procedures and the schools' acceptable use agreements.

If the organisation is operating in school time or when pupils are on site in the care of the school, then the safeguarding of pupils 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**

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.

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 B) that will be given to staff on receipt of equipment from the Network Manager.

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 should return it to the Network Support Department<sup>2</sup> 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 is 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.

### **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 Network etiquette and Privacy**

All staff 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
- BE PROFESSIONAL. Use language and terminology which would normally be used in the classroom
- USE APPROPRIATE LANGUAGE. Remember that a member of staff is a representative of the school and trust on a global public system. Staff may be alone with their computer, but what is

---

<sup>2</sup> For schools with no Network Support staff onsite please return to IT contact within the home school

said and done can be viewed by others. Staff 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 students
- PASSWORD. Staff should not reveal their password to anyone. If staff think 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 students. Staff should NEVER have one to one email with students from their personal email account. Staff should use their school email account (school or school Gmail) to communicate with students and parents, since an audit trail is kept of these messages. This is for their own and student safety. Each secondary school student<sup>3</sup> has an email address issued by the school (Google Mail for Education). This should be used for communication to students and not the student's own personal email address
- PROOFREAD messages to ensure that it is error free and easy to understand
- Messages relating to, or in support of, illegal activities may be reported to the authorities
- SHARING. Resources can now be easily shared with electronically with students via, but not limited to, Google Drive and Classroom. It is the member of staff's responsibility to ensure that the information shared with students 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 student groups to share digital content and ensure that nothing confidential or private is shared with students
- The schools within the AAT provide a variety of online services via their Virtual Learning Environments and these should be the primary source for sharing of content and collaboration with students (for example, Google Drive, Google Mail, Google Classroom, Show My Homework etc.)

## 6.5 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 pupils 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), e-mail 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 students in ANY environment that they would not willingly or appropriately share in a school or school-related setting or in the community.

---

<sup>3</sup> Older primary school children may also have email addresses provided by the school, if not communication is made via parent/carer email addresses

The following examples would be considered to be a breach of AAT policy:

- inappropriate electronic communication with pupils, colleagues and parents/carers, including SMS and instant messaging;
- posting/sending sexually explicit pictures/images to colleagues or pupils;
- 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.

### 6.5.1 Facebook

Where Trust schools maintain a Facebook page as a means to better communicate with pupils and parents, including celebrating successes and notifying parents and students of sports and other upcoming events. Students should not be mentioned by full name and photographs of students will only be used if permission has been granted by a Parent/Carer.

Limited staff will have access to post to this page for example: The Deputy Headteachers, Resources manager and Network Support are responsible for posting to this page.

In terms of staff personal usage of Facebook, the following safeguards are to be observed by all staff. Staff should:

- ensure an appropriate boundary must be set between personal and professional life while using social media. Not exchange private text, phone numbers, personal e-mail addresses or photos of a personal nature with pupils;
- firmly decline student-initiated 'friend' requests from pupils and do not instigate any themselves. Use their own discretion when dealing with friend requests from parents. It is acceptable to decline these invitations and remind parents of more formal channels which they can discuss their child's education;
- realise that pupils will be naturally curious about staff personal lives outside school and may try to find out more about a member of staff. Staff should manage privacy setting and keep them under review. These are particularly important in regard to photos and videos, and remember that no privacy mechanism is 100% guaranteed;
- ensure settings prohibit others from tagging them in any photos or updates without their permission and they can ask others to remove any undesirable content related to them;
- audit and re-evaluate the information about them and who has access to it if they are joining the profession through an Initial Teacher Training route or returning to work after an absence;
- consider that conversations held online may not be private. Be aware of who may have access to what they post – they should only post to 'Friends' by default rather than 'Friends of Friends' and ensure that people on their 'Friends' list are appropriate to view their personal content. Staff should assume that information they post can be accessed and altered;
- not discuss pupils, colleagues, parents or carers online or criticise their employer or others within the school community; respect pupil privacy and confidentiality at all times;
- use strong passwords and change them regularly. Protect their mobile phone/smart phone/tablet computer with a PIN, especially when in school to protect access to its content and potential misuse;
- bring the matter to the attention of a senior leader if they are the victim of cyber bullying or uncomfortable with comments, photos or posts made by pupils of or about them.

## 6.5.2 Twitter

Twitter is a 'micro blogging' platform which allows users to post short text messages. Twitter also allows for the attachment of photos and the embedding of links to other web pages. The main difference between Twitter and email/SMS messaging is that conversations take place in the open rather than in private. This allows for messages to be aimed at a large audience. AAT schools may use Twitter in a similar methodology to the website and Facebook in terms of communicating more effectively with students. However, an increasing number of departments and teaching staff are using Twitter in a pedagogical context, and this has enormous benefits for pupil collaboration and also staff CPD and networking.

The previous advice and policy for Facebook equally applies to Twitter, but there are a number of additional policy statements with respect to this platform:

- Students and Parents/Carers should be encouraged to follow @SchoolName[Department]. E.g. @Ridgeway Academy Geography, @SandringhamPE, @Verulam Media. All Faculty/Department Twitter accounts should follow this naming convention to clearly identify them as being part of the school channels of communication. Network Support need to be notified to update a list of Twitter accounts associated with faculties/staff. Passwords should also be given to Network Support so that continuity can be maintained in the event of staff leaving;
- Specific students will only be mentioned if they have opted to follow a Trust School Faculty Twitter account and mentions of specific students will only be made using their Twitter ID;
- Photographs of students will only be used if a Parent/Carer has granted permission;
- Faculties and staff members are encouraged to tweet links to interesting articles and follow relevant academics and domain experts in order to enrich the curriculum and enhance learning opportunities;
- Open tweets from followers may be replied to and positive debate encouraged;
- Students and Parents/Carers will not be 'followed' by any Faculty account. Furthermore, Faculty Twitter accounts will not be used to send 'direct messages';
- Students should not be allowed to follow staff member's personal accounts. Staff members should consider selecting the 'Protect my Tweets' option in the Privacy settings for Twitter. Protected tweets will be visible only to their approved Twitter followers. Staff members should review their lists of followers and block any current or recent students from their school;
- Care must be taken by staff when expressing political views or controversial opinions, even in the context of encouraging debate and critical thinking. These statements could be misconstrued when taken out of context. Content should only be tweeted if appropriate for a classroom environment and a public setting. Bear in mind that Followers can come from beyond the immediate school community; for example, the Department for Education follows some of the school's official feed.

## 6.5.2 Other social media platforms

There is a proliferation of social media platforms, many of which are very popular with our students e.g. Instagram, Snapchat, WhatsApp etc. The advice above on appropriate use of Twitter and Facebook should be seen as guidance for all current and future social media platforms. 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. Examples of inappropriate behavior on these platforms could include (but not be limited to) participating in WhatsApp group chats with students, following student accounts on Instagram or using picture messaging on Snapchat to communicate with students.

## 6.6 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.

## **6.7 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 locked in a cupboard/filing cabinet, 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 the individual school insurance policy but 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.

## **6.8 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.

## **6.9 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.

## **6.10 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 eyestrain. 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.



## 6.11 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.

## APPENDIX A – AAT Model policy for Online Safety Including Online Safety Acceptable Use Agreements

	<b>IT – Acceptable Use: Appendix A Online Safety (Including Online Safety Acceptable Use Agreements)</b>	
	<b>Last reviewed:</b> May 2021	<b>Next Review:</b> May 2022

### 1 PRINCIPLES

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 pupils, 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 pupils 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.

### 2 TRUST ARRANGEMENTS

The Alban Academies Trust (AAT) has adapted the Herts for Learning (HfL) Online Safety Policy to create this model policy for all of the schools within the Trust.

### 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 an online safety lead.

All breaches of this policy must be reported to the school's online safety lead.

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 pupils are on site in the care of the school, then the safeguarding of pupils is paramount and the organisation must adhere to the school's online safety procedures and acceptable use agreements.

## 4 SCOPE OF THE POLICY

The policy applies to:

- pupils
- 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 pupils 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.

## 5 POLICY AND 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 pupils, parents/carers, staff, governors and trustees and all other visitors to the school.

### 5.1 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 pupils, parents or conduct any school business using a personal email address. Pupils 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 pupils should not open emails or attachments from suspect sources and should report their receipt to the school Network Manager<sup>4</sup>.

---

<sup>4</sup> For schools with no Network Support staff onsite please report to IT contact within the home school

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

## **5.2 Visiting online sites and downloading**

- Staff must preview sites, software and apps before their use in school or before recommending them to pupils. Before using any online service that requires user accounts to be created or the sharing of any personal data, staff must consult with the Network Manager 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 pupils 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 school's online safety lead.

### **5.3 Storage of Images**

Photographs and videos provide valuable evidence of pupils' 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 GDPR policy for greater clarification).

Photographs and images of pupils 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 school's online safety lead. Staff and pupils 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 pupils, must only use school equipment to record images of pupils 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.

### **5.4 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 mobile/personal devices in a school context is educational.

The school allows the following use of mobile technologies:

	School devices			Personal devices		Staff (including temporary and peripatetic) owned	Visitor owned
	School owned and allocated to a single user	School owned for use by multiple users	Authorised device <sup>5</sup>	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		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
- 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)

<sup>5</sup> 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.

- 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.

#### New technological devices

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

#### **5.5 Reporting incidents, abuse and inappropriate material**

There may be occasions in school when either a pupil or an adult receives an offensive, abusive or inappropriate message or accidentally accesses upsetting or abusive material. When such a situation occurs the pupil or adult must report the incident immediately to the first available member of staff, the DSL, the headteacher. These incidents need to be reported on the schools Online Safety Log. Where such an incident may lead to significant harm, safeguarding procedures should be followed. The school takes the reporting of such incidents seriously and where judged necessary, the DSL will refer details to social care or the police.

## **6 CURRICULUM**

Online safety is fully embedded within our curriculum. The school provides a comprehensive age appropriate curriculum for online safety which enables pupils to become informed, safe and responsible. This includes teaching to prevent radicalisation, for which staff provide a narrative to counter extremism. The Personal Development 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 pupils 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. Pupils are taught to recognise the creative, collaborative, cultural, economic and educational opportunities provided by the internet, mobile and digital technologies. Curriculum work will also include areas such as:

- Understanding how to use the internet, mobile and digital technologies in a balanced and appropriate way to avoid negative impact on wellbeing, e.g. regulated screen time and diverse online activity
- Learning how to develop a positive online reputation and enhance future opportunities e.g. in relationships and employment
- Developing critical thinking skills and the confidence to challenge and question what they see and read in relation to online content e.g. recognising fake news and extremism, understanding commercial manipulation, maintaining an authentic sense of self that is resilient to online

pressure, learning how easy it is to lie online (i.e. users may not be who they say they are and may have ulterior motives) Understanding the dangers of giving out personal details online and the importance of maintaining maximum privacy online

- Thinking carefully before placing images online and considering their appropriateness and understanding the importance of gaining consent before posting photographs of others
- Understanding the permanency of all online postings and conversations
- Understanding relevant legislation, including copyright, and the importance of respecting other people's information, reputation and images.
- Understanding the importance of online respect and what constitutes cyberbullying, how to avoid it, the impact it has and how to access help.
- How the law can help protect against online risks and abuse

## **7 STAFF CPL**

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 (Appendix II) as part of their induction and before having contact with pupils.

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 (Appendix II)

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 (Appendix II).

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

## **8 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 VI. The Acceptable Use Agreement explains the school's expectations and pupil and parent/carer responsibilities.



## 9 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 pupils and staff are minimised.

All breaches of this policy must be reported, and all reported incidents will be logged in the Online Safety Log (see appendix IX). All staff have the individual responsibility to ensure that incidents have been correctly recorded, acted upon and reported.

The school supports pupils 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.

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.

## 10 APPENDICES OF THE ONLINE SAFETY POLICY

- I. Online Safety Acceptable Use Agreement - Staff, Governors and student teachers (on placement or on staff)
- II. Online Safety Acceptable Use Agreement - Peripatetic teachers/coaches, supply teachers
- III. Requirements for visitors, volunteers and parent/carers helpers working in the school (working directly with children or otherwise)
- IV. Online Safety Acceptable Use Agreement Primary Pupils
- V. Online Safety Acceptable Use Agreements Secondary Pupils
- VI. Online safety policy guide - Summary of key parent/carer responsibilities
- VII. Guidance on the process for responding to cyberbullying incidents
- VIII. Guidance for staff on preventing and responding to negative comments on social media
- IX. Online safety incident log

## **Appendix I - 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 school online safety lead. 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 online safety lead 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 pupils and/or parents/carers.

### **Social networking**

I understand the need to separate my professional role from my private friendships; in my professional capacity I will not become 'friends' with parents/carers or pupils on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils.

When using social networking for personal use I will ensure my settings are not public. My private account postings will never undermine or disparage the school, its staff, governors, trustees, parents/carers or pupils. Privileged information must remain confidential.

I will not upload any material about or references to the school or its community on my personal social networks.

## **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 only upload images or videos of staff, pupils or parents/carers onto school approved sites where specific permission has been granted.

I will not take images, sound recordings or videos of school events or activities on any personal device.

## **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 that as a member of staff 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, pupils or parents/carers) to the DSL.

### **Classroom management of internet access**

I will pre-check for appropriateness 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 pupils. I will also check the appropriacy 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.

### **Video conferencing**

I will only use the conferencing tools that have been identified and risk assessed by the school leadership, DPO and DSL. A school-owned device should be used when running video-conferences, where possible.

### **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 II - Online Safety Acceptable Use Agreement - Peripatetic teachers/coaches, supply teachers

School name: <<enter school name>>

Online Safety Lead: <<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 online safety lead 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 pupils 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 the need to separate my professional role from my private friendships; in my professional capacity I will not become 'friends' with parents/carers or pupils on social networks. Where my school role is my only connection to an individual, private online contact is unacceptable with parents/carers or pupils.

Information can be shared with pupils over 13 and parents/carers through an organisational social network site/page e.g. on Facebook or Twitter, but never through a personal account or site. In my professional role in the school, I will never engage in 1-1 exchanges with pupils or parent/carers on personal social network sites.

My private account postings will never undermine or disparage the school, its staff, governors, trustees, parents/carers or pupils. Privileged information known as a result of my work in the school must remain confidential.

I will not upload any material about or references to the school or its community on my personal social networks.

## **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, pupils 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, pupils 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 pupils.

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.

### **Video conferencing**

I will only use the conferencing tools that have been identified and risk assessed by the school leadership, DPO and DSL. A school-owned device should be used when running video-conferences, where possible.

### **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 III - Requirements for visitors, volunteers and parent/carer helpers (Working directly with children or otherwise)

School name: <<enter school name>>

Online Safety Lead: <<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 pupils. 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 pupils, 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 pupils. 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.



### 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, pupils 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 V - Online Safety Acceptable Use Agreement Secondary Pupils

- 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 user name 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 report immediately 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.
- 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 VI - Online safety policy guide - Summary of key parent/carers 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 pupils.
- 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/carers 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 pupils 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/carers, 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, pupils and parents/carers.

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

## Appendix VII - Guidance on the process for responding to cyberbullying incidents

All cyberbullying incidents should be reported and responded to. Where the perpetrator is a member of the school community the majority of cases can be dealt with through mediation and/or disciplinary processes.

The following procedures are recommended:

- Never reply to the sender/poster of cyberbullying content. If applicable, block the sender.
- Incidents should be reported immediately. Pupils should report to a member of staff (e.g. class teacher, headteacher) and staff members should seek support from their line manager or a senior member of staff.
- The person reporting the cyberbullying should save the evidence and record the time and date. This evidence must not be forwarded but must be available to show at a meeting. Under no circumstances should indecent images of children and young people be printed or forwarded as this is a further criminal act. Staff should not ask to see the evidence of reported indecent images of children or young people but must refer this immediately to the police. Any member of staff being shown such evidence should immediately inform their line manager or the headteacher so that the circumstances can be recorded.
- A senior member of staff will meet with the person who has reported the incident and the target, if different, to listen, reassure and support. All relevant facts will be reviewed and documented.
- A senior member of staff will conduct an investigation.
- Anyone found to have cyberbullied will have attention drawn to the seriousness of their behaviour and if necessary, the police will be involved. If the comments are threatening, abusive, sexist, of a sexual nature, constitute a hate crime or are libelous they may well break the law. Online harassment and stalking is also a crime.
- Once evidence has been secured then the person who has cyberbullied will be requested to remove the offending comments/material. Any refusal will lead to an escalation of sanctions.

## Appendix VIII - 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 libelous 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 re-iterate the seriousness of the matter.

# Appendix IX – Example Online Safety Incident Log

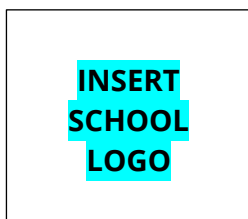
## Example Online Safety Log

As per DfE guidelines, the school has a duty to keep a log of all online safety incidents that have involved a significant investigation or sanction being issued. Tutors, PDs, Pastoral Support Staff or LG member should record details in this Google Sheet. Details do not need to be extensive, but a clear overview of the incident and actions undertaken should be given. The "student name" field should capture the name of the student who reported the incident. Please review the examples given below.

Student Name	Tutor Group	Incident Date	Incident Details	Actions and Outcome	Staff Initials	LG Acknowledged
Joe Bloggs	8A	05/05/2020	Joe reported to MAL that he had repeatedly received emails from JH (BT) over the past few weeks saying that he would jump Joe after school. Joe showed the emails to MAL.	MAL spoke with JH about his conduct whilst using school email. JH's parents were informed about the incident. The threatening and persistent nature of the emails led to a CA being issued.	MAL	TRUE
Sarah Jones	11F		Sarah had said that she had received a Snapchat message from an unknown adult which contained an image of the man's penis. As the message was sent via Snapchat she no longer had the photo in question. Sarah said she accepted the person as a friend on Snapchat but never spoke to him. The Snapchat username was "StkAbansDngOnaChallenge".	TRB inform Sarah that this was a police matter as an adult has sent an inappropriate image to a minor. Whilst Sarah has opted, she understands the risks of Snapchat. TRB was informed her about the incident. Mrs Jones was asked to call the police on 101 to report the incident. TRB called back the next day to confirm this had been done. Sarah reminded about the dangers of adding strangers to social media platforms.	TRB	TRUE
Abdul Khan	10T	11/07/2020	Abdul reported to STK that HF (10S) had been added to a WhatsApp group chat which is used for promoting the sale of recreational drugs in St Albans and Herts. Abdul was nervous about informing STK about this as he didn't want to be a "rat".	STK spoke to HF about the concern raised. HF first denied he was in such a WhatsApp group but when STK asked to see his phone he admitted he was in the group. STK saw the contents of the group. Brown & White Tng were identified as the person who had added HF's parents into school to talk to them about the incident. STK called the police on 101 to report the WhatsApp group. In a conversation with HF he stated "I ain't purchased anything from there, I don't do drugs, but it is proper cheap" - see safeguarding concern on Bromcom.	STK	TRUE



## APPENDIX B - Staff Responsibility Agreement



### STAFF RESPONSIBILITY AGREEMENT

As a member of staff at <<enter school name>>, you may be issued with a number of important items or loaned equipment for which you will be responsible. These may include:

- Laptop & associated materials (cables and charger, carrying case etc.)
- Digital cameras
- Keys for subject rooms & cupboards/store rooms/teaching block

The items are issued under the following conditions:

1. The items remain the property of <<enter school name>> and are for use ONLY by the named member of staff. You should not use items for any purpose which would contravene reasonable expectations for the conduct of an employee of the school.
2. The laptop computer is insured under the school insurance policy, but all reasonable precautions should be taken to ensure the security of the machine and the (sometimes sensitive and confidential) data held on it. It is NOT reasonable to leave the item in an unattended vehicle nor in an unlocked room in school. **If you are found to be negligent you will be required to pay for a replacement of the item lost or damaged. A new laptop will cost approximately £400.**
3. You must take reasonable steps to ensure that the items can be returned to the school in a fit state for a subsequent user. All software installed must be **fully** licensed.
4. You will be required to return all items, laptop and iPad with chargers, by your last teaching day at the school.

**Personal property, including cars, brought onto school property is your own responsibility. You are advised to check your personal insurance before bringing personal property onto premises.**

Please complete the form below and return it to <<ENTER NAME>> - Network Manager.

Name: \_\_\_\_\_

I agree to abide by the above conditions and will notify a member of the SLT/Leadership Group immediately if an item is lost.

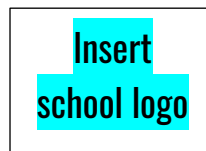
In addition, if I mislay my keys, I will contact the SLT/Leadership Group immediately.

Signed: ..... 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.

1. 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.
2. 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.
3. 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.
4. When transporting your computer always turn it off and put it in a carrying case, other than between lessons.
5. 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.
6. Keep all liquids away from your laptop. Almost any liquid spilt on the computer will result in it being completely unusable.
7. Keep your laptop away from magnetic fields. Magnetic fields can erase data on hard drives.
8. 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)
9. 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.
10. Staff must not use or install unlicensed, malicious or gaming software.
11. You must not create documents or files for which storage would contravene the Data Protection Act.
12. Any material on the laptop must be in accordance with the law.
13. 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.
14. 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.
15. 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.
16. 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.



## SCHOOL STAFF TABLET LOAN AGREEMENT

### Bring your own device project

<<insert school name>> has a programme to allow students to bring their own devices to use in class to enhance learning. You are a person to whom a tablet should be loaned in order for you to partake in the project, become familiar with the device and develop ways to use devices in delivering your lessons to improve student outcomes.

**Please read, then sign and date the agreement in the box below to indicate your acceptance of the terms herein:**

While the tablet is in your care the following items should be noted:

1. The tablet device and case and charger remain the property of <<insert school name>> and are only for the use of the member of staff it is issued to. They must be returned to the school on request.
2. Insurance cover provides protection from the standard risks but excludes accident, damage and theft from an un-attended car. If the tablet is stolen from an un-attended car, you will be responsible for its replacement.
3. You are free to use the device as you wish including the choice and download of software and Apps, however the appropriateness must be considered (please refer to the AAT IT Use Policy); it should not compromise professionalism nor cause risk to the device.
4. You should create your own school Apple ID as instructed and use this to manage the apps on the device and keep them updated. We recommend that you install iTunes on your school laptop and keep your account for managing the school iPad separate from any personal account used to manage your own devices.
5. The school will provide a base set of apps (e.g. Office 365 and a variety of teaching apps.) Apps that are specific to your faculty will need to be funded from the faculty budget and no other costs are chargeable to the school.
6. Should any faults occur, the school’s Network Support staff must be advised as soon as possible so that they may arrange any necessary repairs. Do not attempt to fix suspected hardware faults yourself.
7. You should make reasonable efforts to use the device for Teaching and Learning purposes – the school expects you to use the tool for professional development and curriculum enrichment (not just Angry Birds!)
8. This tablet must be kept secure and remain passcode protected or biometrically secure at all times. Particular care needs to be taken over sensitive student or school data stored on the device or in cloud-based services.
9. The terms of the AAT IT Acceptable Use & Online Safety Policy extend to use of this tablet and must be adhered to – this includes appropriate use, password and data protection, technology misuse, recording and storing of images/videos, communicating via social networks and health and safety. Violation of these terms is likely to result in loss of access and disciplinary action in accordance with <<enter school name>>’s Disciplinary Procedures.
10. On return your iPad must have your iCloud account removed or you could be liable to pay the appropriate cost for a replacement.

**Tablet Make:**

**Serial Number:**

**Authorised by: (signature)**.....

**Date**.....

**Name of Member of Staff :**

I agree to follow this agreement and to support the safe use of ICT throughout the school.

**Signature** .....

**Date** .....

**Faculty** .....