



Alleyne's School Policies & Procedures

Information Technology (IT) and e-Safety Policy

Name of Policy	Information Technology (IT) and e-Safety Policy
ISSR	Part 3: Welfare, Health and Safety of Pupils and other legislation
Reviewed by	SLT
Author/SMT	Mr AWA Skinnard, Senior Deputy Head
Date of school review	September 2023
Date of next school review	September 2024

Policy Overview

This policy applies to the Senior School and the Junior School.

Introduction

Alleyne's makes use of a wide variety of electronic data platforms in its daily use. From administrative support, to teaching resources and communication channels, pupils and staff at Alleyne's have many opportunities afforded to them by access to, and use of, information technology (IT).

With such use comes great advantages for a school community, but it also poses a need for an agreed protocol for use of IT, which this policy aims to address.

This policy gives an outline of the staff management of the IT facilities and the expectations of use of these facilities by staff and pupils.

This policy also outlines the educational support of pupils' IT use within the curriculum, and through the pastoral management of pupils at Alleyne's.

The policy has been drawn up with regard to the statutory duty all schools are under to implement safe practices in support of safeguarding of all pupils. The School takes active steps to warn pupils about the risk of harm posed by misuse of digital devices and social media, in terms of peer abuse perpetuated by cyber-bullying. The School also takes active steps to mitigate against the possible use of IT with dangers of radicalisation and being drawn into possible terrorist activity, and reflects the guidance for all schools under the Prevent guidance given by the government (see *Keeping Safe in Education* (Sep 2023)).

IT resources at Alleyn's

The School provides a wide variety of information technology equipment, systems and services.

- Physical equipment, including but not limited to computers, laptops, Surface Pro devices, iPads, mobile telephones, AV equipment, digital cameras (still and video), sound recording equipment, and the associated infrastructure of the computer and wireless network;
- Software, systems and apps for use by pupils and staff in school;
- Web-based systems for use by pupils, staff and parents, either in school or from home or any other web-enabled location or device, hosted either locally or externally.

IT management and oversight

The School will ensure, through internal documentation and procedures, that IT systems are provided and managed in an effective and professional manner.

The School has an IT Strategy Committee which deals with all issues relating to IT planning, purchasing and use.

In line with *Keeping Children Safe in Education* (Sep 2023), the Designated Safeguarding (DSL) takes lead responsibility for the safeguarding and child protection aspects of IT use at the School, including online safety and understanding the filtering and monitoring systems and processes in place. The DSL arranges that staff are trained in online safety (which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring) at induction. The training is regularly updated for all staff.

The DSL works with appropriate IT staff and with the Link Governor for safeguarding in auditing the filtering and monitoring systems' effectiveness, and in overseeing the pursuance of online safety at School with other relevant colleagues.

The Governing Body, thus, ensures there is appropriate filtering and monitoring in place. In this responsibility they must ensure that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding.

The School pays regard to the standards published by the Department for Education which set out that schools should:

- identify and assign roles and responsibilities to manage filtering and monitoring systems
- review filtering and monitoring provision at least annually
- block harmful and inappropriate content without unreasonably impacting teaching and learning
- have effective monitoring strategies in place that meet their safeguarding needs.

The standards can be read [here](#).

The School's Safeguarding and Child Protection Policy contains details of the School's systems for filtering and monitoring, as well as other aspects of online safety under the leadership of the DSL. See Appendix 3.

For a list of personnel with specific IT responsibilities, see Appendix 1.

Purchasing recommendations regarding new equipment, software or services will be undertaken by the IT Strategy Committee and will include appropriate due diligence on products and suppliers to ensure that the needs of the School are met. Under no circumstances should departments buy IT equipment or software without prior authorisation from the Director of Strategic Projects and the Head of IT Systems and Services, even if items are charged to the departmental budget. Of particular importance are security, management and data protection issues, addressing our existing policies on safeguarding, data protection and our acceptable use policies.

Safeguarding & Prevent

School systems will be selected, designed and managed so as to aim to prevent inappropriate material from the internet being available to pupils, or seen by staff, in school. In this aim, and on the instruction of senior staff responsible for safeguarding, the IT Support team can investigate the IT use of pupils and staff in School, and view web searches, emails, documents and other digital activity on School equipment.

Our Safeguarding policy makes clear the action which staff should take if they believe that unsafe or inappropriate activity is taking place either on School equipment, or in school by pupils using their own devices, or by staff.

The issues of e-safety and cyber-bullying are raised with pupils through their signing of agreement to the pupil Acceptable Use Policy, through the PSHE programme (which includes visiting speakers on e-safety), and through communication with parents drawing their attention to what their children sign in agreeing to our Acceptable Use Agreement.

Relevant matters to do with e-safety are also raised in the training of staff members, who have all completed an online course on *Keeping Children Safe in Education* (Sep 2023) and an introduction to prevent guidelines issued by government in periodic staff training. Our duty of care under the Prevent legislation is raised in the Staff IT Acceptable Use Agreement.

Data protection

The Chief Operating Officer has responsibility for data protection.

Software and services will be selected to ensure that the requirements of our Data Protection Policy, (recently re-written to be in line with the new GDPR (May 2018)) can be met.

In addition to our Data Protection Policy, the School will ensure that use of external software and service providers meets our own criteria for maintaining the security and integrity of personal data, and data confidential to the School.

IT Acceptable Use Policies for pupils and staff and for the awareness of parents

All users of school IT systems sign the Acceptable Use Policy (AUA) relevant to their use. Teaching staff sign an Acceptable Use of IT Policy which all other staff and all pupils must sign. All the AUAs include reference to which sets out the way in which school IT equipment and systems may be used. AUAs for pupils and staff are signed each academic year.

Senior School pupils sign their agreement on the Hub, and parents acknowledge an Alleyn's Post email to show their agreement with, and support of, the School policy signed by their child. The AUA for pupils includes reference to use of appropriate internet and social media pages, in line with the Prevent guidance issued to schools, as well as reference to peer abuse which can occur on social media and through use of digital facilities. Junior School pupils sign their agreement in their day books.

Staff working in IT Support, and others with access to personal information about staff, pupils or parents, also sign an Acceptable Use Agreement which regulates the legitimate accessing of the personal information of others, and the way in which they may access such data, both for their own protection and the privacy of others.

Blended Learning and Surface Pro use in teaching and learning

Alleyn's is developing the use of IT platforms to support learning both in and out of the classroom. Senior School staff who use such technological support in their lessons sign an Acceptable Use agreement for the Surface Pros used in teaching, and the pupil AUP includes reference to the need for appropriate use of devices in learning settings. The senior pupil AUA also covers bring your own device (BYOD).

Monitoring the effectiveness of the policy

The Head of IT Systems and Services and the Director of Strategic Projects will work closely with the Senior Deputy Head, who is the DSL, and with the Chief Operating Officer, who is the Data Protection Officer, with the aim of ensuring the policy achieves its aim of providing a safe environment for the use of IT at Alleyn's. There is also oversight from the Link Governor for safeguarding.

This will be achieved by:

- regular meetings between the Director of Strategic Projects, the Head of IT Systems and Services and the Chief Operating Officer;
- the compilation of an e-safety incident log;
- the e-safety incident log being a standing agenda item for IT Strategy Committee meetings;
- regular monitoring of more general e-safety matters at the IT Strategy Committee;
- Checking for trends by the Director of Strategic Projects and the Chief Operating Officer;
- the e-safety incident log featuring in the annual audit with the Link Governor for safeguarding and in regular reports at Governors' Board meetings;
- regular consultations with pupils (*eg* through the Learning Council, the School Council, questionnaires on The Hub and PSCHE lessons);
- the work of Digital Leads under the leadership of the Head of Digital Learning and Innovation;
- an annual audit of IT and online safety, including checking of filtering and monitoring, in conjunction with the Link Governor for safeguarding and the DSL.

The use of digital images

Parents may request that no image of their children be used in any outward facing electronic platform (*e.g.* the website), but images of staff and pupils may be published on the Hub, which is only accessible

to members of the Alleyn's community of staff, pupils and parents. The whole community is regularly reminded of the importance of not sharing content from the Hub with any wider audience. It is an expectation that staff should download within 24 hours – or within 24 hours of return from a trip lasting longer than a day – any digital images of children at the School that are recorded on personal devices. Such images, after being downloaded, should be deleted so the member of staff is no longer in possession of them. Images of EYFS (Reception) children must only ever be taken with school devices.

Misuse of Alleyn's IT systems or social media in or outside school

Staff are regularly reminded of the need for careful use of any social media with work at school. The Director of External Relations and her staff offer guidance to staff in any use of social media in promoting the School. In the Staff Code of Conduct, in the Staff Handbook, and with regular announcements at Staff meetings, there are reminders about appropriate use of IT. Members of staff are advised not to contact pupils directly through personal email addresses, or other electronic forums (except in their performance of school activities, *e.g.* House activities on Facebook) and may only use School email addresses for individual, direct contact.

Inappropriate use of school IT systems or social media may result in disciplinary procedures being instituted.

Pupils are subject to normal disciplinary action should they break the AUP.

Relevant school policies in support of safe use of IT by staff and pupils include:

- 22-23 IT and E-safety Policy
- 22-23 Acceptable Use Policy for Pupils using School IT facilities;
- 22-23 Acceptable Use Policy for Staff using School IT facilities;
- 22-23 Safeguarding and Child Protection Policy.

APPENDIX 1

ROLES AND RESPONSIBILITIES FOR IT MANAGEMENT AND ONLINE SAFETY INVOLVING SCHOOL DEVICES AND SCHOOL NETWORKS

DESIGNATED SAFEGUARDING LEAD (DSL)

The DSL has responsibility for understanding the filtering and monitoring systems and processes in place. The DSL leads on the induction and training of staff. At induction, staff will receive appropriate online safety guidance as part of their safeguarding and child protection training, including ensuring an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring. Staff receive regular training updates.

DIRECTOR OF STRATEGIC PROJECTS

HEAD OF IT SYSTEMS AND SERVICES

HEAD OF DIGITAL LEARNING AND INNOVATION

LINK GOVERNOR FOR SAFEGUARDING

APPENDIX 2

ACCEPTABLE USE AGREEMENT FOR PUPILS USING SCHOOL IT FACILITIES:

This agreement applies to pupils in the Senior School.

Pupil e-Safety Agreement (including use of home/personal devices on School premises and use of School wi-fi)

1. I will only use the School's computers and other digital devices for schoolwork and homework.
2. I will not use School ICT facilities within school or any other IT facilities outside to break the Anti-bullying Policy or Pupil Code of Conduct and am aware of the potential legal consequences.
3. I will not access, create, download, copy, print or distribute any material that may be considered to be racist, sexist, obscene, violent or bullying, or make derogatory or hurtful comments about other pupils and/or staff. I will not participate in any activity that can be reasonably classed as cyber-bullying (repeated activity intending to hurt others). I will not bring the School into disrepute by any use of the internet or social media on or off the School site.
4. I know that I am fully responsible for all comments I make or content which I create on the Hub and on Teams, for the content of any email I create or send, as well as the content of any files in my possession or in my user area.
5. I understand that when using school approved group messaging services such as Microsoft Teams that all messages are moderated and anything inappropriate or offensive will be the subject to sanctions.
6. I am aware that the school uses software that can identify when inappropriate or offensive words or phrases are typed into school computers.
7. I will not share information from school IT systems (including screengrabs, and material from the Hub) outside the School, or on any form of social media.
8. I will not attempt to visit internet sites that I know to be banned by the School.
9. I must not attempt to circumvent the Internet Filtering system in any way. This includes the use of a VPN.
10. The use of social networking sites and the playing of games outside of authorised clubs and societies is forbidden.
11. I will not access any chargeable Internet services, nor buy, nor offer for sale, any item over the Internet, the Hub, tablet device or by email.
12. I will keep secret my own user ID and password and will not log on with anyone else's user ID and password.
13. I will not give out personal details such as my name, address, photograph, telephone number, bank account or credit card details, on the Internet, the Hub or by email.
14. I will not open an email attachment, or download a file, unless I know and trust the person who has sent it.
15. I will not capture any images of other people, either at the School or outside (if there is a risk of their happiness at school being compromised), without their permission, and will never distribute images of other people on social media or the internet without their consent (this includes time when not at school).
16. I understand (according to *Keeping Children Safe in Education* (Sep 2022)) that, consensual and non-consensual sharing of nude and semi-nude images and/or videos and taking and sharing nude photographs of U18s is a criminal offence.
17. I will not participate in any activity on the School IT network that runs the risk of my being drawn into extremism – this falls under the duties set out for schools to protect children "...from the risk of radicalisation". [From *Keeping Children Safe in Education* (September 2022). This is covered in the PSHE programme at school and members of staff are available for discussion about any concerns in this area.]
18. You may bring your own devices for use in lessons and connect to the school Wi-Fi. However, you must adhere to the rules stated in this document.
19. When I use a mobile device of my own in school (under appropriate supervision from a member of staff) I will abide by the Code of Conduct for use of such devices published on the Hub in the 'IT Support' section.
20. I will not download files and install programs or scripts of any kind on any School computer or tablet device, or any other person's devices.

21. I will not bring in a USB or other portable hard drives but will instead use the One Drive provided by the School.
22. I will only edit or delete files in my user area and will not encrypt or password protect them.
23. I will not save files onto School devices and will delete any content made at the end of the lesson unless instructed not to do so.
24. I will behave sensibly in computer rooms and treat the equipment with respect.
25. I will not take food or drink into any of the computer rooms.
26. I will report any faulty or broken equipment to a member of the IT Support staff as soon as possible.
27. I will not use classroom technology without a teacher present. (This includes the teacher PC, whiteboard, projector, interactive screen, television and any mobile devices or technology provided for the use of the teaching staff.)
28. I am aware that the use of any School computer, tablet device, classroom technology, telephone or communications facility for any unauthorised activity is against School policy and may even be a criminal offence.

Online Safety: General reminders

- You should not share ANY personal contact information or images online
- You should be mindful of who you are speaking to online and speak to a teacher or your parents if you are concerned
- Ensure your privacy settings are set correctly.

By clicking the submit button below, you confirm that you have read and agree to abide by the above pupil e-safety agreement and acceptable use policy.

I have read and understand these rules and agree to them.*

NAME:	
FORM:	
SIGNED:	
DATE:	

*electronic signature for pupils is obtained via the Hub.

APPENDIX 3

ACCEPTABLE USE AGREEMENT FOR STAFF USING SCHOOL IT FACILITIES

This policy applies to the whole Alleyn’s School staff community, including the Junior and Senior Schools.

Section 1 of this policy applies to all staff. Section 2 of this policy applies to all staff issued with a Surface Pro or laptop to support their work at the School.

SECTION 1 - Staff Laptop, Surface Pro, Desktop computer, iPad and mobile device (school or personally-owned) usage

It is subject to the *Acceptable Use Policy* including the limitations on personal use. A School-owned computer should not be used by anyone except the registered user. Using a personally-owned mobile device like a phone or a tablet with the School wi-fi provision is also subject to the *Acceptable Use Policy*.

General

The primary purpose of the provision of School IT equipment and network access is as a resource for teaching, learning, research, organisation and other approved business activities of the School. The School reserves the right to monitor IT usage including access to the Internet and emails in order to ensure compliance with the *Acceptable Use Policy* and current legislation.

Safeguarding & Prevent

School systems will be selected, designed and managed with the aim of preventing inappropriate material from the internet being available to pupils, or seen by staff, in school. In this aim, and on the instruction of senior staff responsible for safeguarding, the IT Support team can investigate the IT use of pupils and staff in School, and view web searches, emails, documents and other digital activity on School equipment.

Our Safeguarding policy makes clear the action which staff should take if they believe that unsafe or inappropriate activity is taking place either on School equipment, in school by pupils using their own devices, or by staff. It is also a matter of safeguarding importance if a member of staff is concerned about the digital behaviour of a pupil outside school and the concerns should be passed to the relevant DSL/DDSL.

Members of staff may not communicate personally with pupils on email or using social media applications (*eg* Facebook, Teams, Instagram) in a way that is inconsistent with the School's Child Protection and Safeguarding Policy. If a member of staff is communicating with a pupil by email or Teams, the member of staff should use the School email address of the pupil. If there is occasion to contact the pupil using a different email address, then the parents must be copied in to that communication.

Members of staff must pay due regard to the School's guidelines on use of photography and video, as outlined in the Child Protection and Safeguarding Policy.

Members of staff must report any concerns they come across in line with the Prevent duty, under which all schools must operate. This includes a concern that a pupil is being drawn into any form of radicalisation that might lead to the pupil coming to support terrorism and extremist ideologies associated with terrorist groups.

Security

Passwords are the primary security mechanism for maintaining the integrity of the network and all activity is logged against each user's password-protected session. Staff are responsible for the content of emails that are sent from their account, for the content of material in their 'work' areas or placed in shared areas and for any printed or other output produced using their network user identity. It is essential therefore that passwords are not divulged to anyone, unless asked to by a member of the IT staff in order to perform maintenance or support. Staff must select suitably complex passwords and change them when required to do so by the system. All Alley'n's staff must have Multi-factor Authentication (MFA) enabled on their Office 365 accounts.

No attempt should be made to bypass the folder access or other security mechanisms which are in place across the file servers. Staff requiring access to a new area should contact the IT support staff. Staff should also not attempt to circumvent the School's internet filtering system. For example, using a VPN.

Staff should not use USB or external hard drives in School (except under exceptional circumstance cleared in advance with the IT Support team. If they are used they should be encrypted). All staff should use OneDrive to store files they would like to access outside school. USB pen drives, external hard drives and similar devices must not be

used to install software onto machines. Staff should be aware that some viruses can spread via data files (eg Word, Excel, PDF) and files from unknown or untrusted sources should not be introduced onto the School network. IT support staff can check such files if required.

Staff should not use other personal cloud service accounts to store confidential pupil information. Staff must use their organisational OneDrive account to handle documents for School business. However, they should not synchronise their OneDrive with their own computers (as this creates a copy on the local computer).

Software

Staff must not install software, however obtained, onto School IT equipment either locally or on the fileserver without the approval of the IT Manager. This is both to maintain the network integrity and to ensure compliance with copyright and licensing. Equally, staff should not remove or re-configure any of the pre-installed software on any IT equipment without the consent of the IT Manager. The use of apps on school tablet devices is dealt with separately in the Tablet Acceptable Use Policy and in guidance on the Hub.

Email

Staff should be aware that email attachments may contain viruses. IT support staff are available to investigate email attachments from unknown or unsolicited sources if required. Staff should also be aware that all emails are suffixed with a School disclaimer and that the content of emails can be monitored. Sometimes, staff may receive emails seemingly sent by colleagues, but may on closer inspection not be genuine emails and may contain unexpected attachments or links to phishing sites. Staff should be vigilant and report any unexpected emails to IT support staff. Emails can be used for any communication purposes but should not be used:

- for the transmission of unsolicited, commercial or advertising material, chain letters, press releases, or other junk mail ('spam') of any kind to other users or organisations;
- for the unauthorised transmission to a third party of confidential material concerning the activities of Alleyn's School;
- for the transmission of material such that infringes copyright or intellectual property rights;
- for the use of impolite terms or language, including offensive or condescending terms;
- for criticising individuals, including copy distribution to other individuals;
- for the creation or transmission of material which brings the School into disrepute;
- for any private communication with pupils at the School.

The School Management will exercise its discretion in judging reasonable bounds for acceptability of material transmitted by email.

Personal Use of School IT equipment (see also use of School-issued laptops or Surface Pros below)

Although the primary purpose of the School's IT equipment is as an academic resource, in practice, a very limited use for personal purposes is regarded as acceptable provided that:

- it does not conflict with an employee's obligations to Alleyn's School as employer;
- it is not at a level detrimental to the primary purpose for which the facilities are provided, in particular the fileserver should not be used for the storage of large amounts of personal files;
- priority is given to users who require resources for the primary purpose;
- it is not of a commercial or profit-making nature;
- it is not of a nature that competes with the School in business;
- it does not conflict with any of the School's rules, regulations or policies.

Microsoft Teams and Other Forms of Communication

If staff are using Microsoft Teams or other similar services that offer group chats between staff and students, it is important that group conversations are moderated. If a group is set up in Teams for example it should be the

responsibility of the team owner to ensure that anything inappropriate is recorded using a screenshot and then the offending message is deleted. The School's safeguarding policy and code of practice for staff should be followed when dealing with these kinds of incidents. The School's IT Team can retrieve private Teams chat or posts in a Team should they be required to.

Data Confidentiality

In the course of their duties staff may have need to access data held on the School's Management Information System. Data accessed in such a way should be treated as confidential and only processed in accordance with School procedures. Access to confidential information without due cause and/or distributing any such information to third parties will be considered a serious breach of the terms and conditions of employment. Guidance for the access, management and retention of data is given separately on the Hub in light of GPDR (May 2018). Staff must refer to the Hub for compliance with the expectations at Alleyn's of handling data.

Miscellaneous

Staff may not create, download, copy, print or distribute any material that may be considered to be racist, sexist, obscene, violent, bullying or likely to cause annoyance, inconvenience offence or needless anxiety. Staff should not use IT equipment to engage in any activity which is in contravention of current legislation including but not limited to discriminatory activity.

Care should be exercised when recording information about the School on social networks or other public forums. Contributions to online forums, discussion groups, blogs or other social media must be phrased so that they do not compromise or undermine the name or reputation of Alleyn's School.

Staff may not access any pay-per-view or chargeable internet services, nor access any internet chat rooms of any nature.

Staff should avoid consuming food or drink when using IT equipment. Not only does this risk damaging the equipment, but research has shown that keyboards and mice can harbour significant levels of bacteria.

Section 2: For staff users of School-issued laptops and Surface Pros:

A school device, laptop, iPad or Surface Pro computer is a mobile extension of the School network and remains the property of the School.

When laptops are not connected to the School's network for a period of time they become more vulnerable to attack from viruses, malware, spyware *etc*. It is therefore recommended that laptops are connected to the School's network at least once a week during term time. If a laptop or Surface Pro user has any reason to think that their machine has been compromised in any way then they must not connect it to the School network and should immediately refer to the IT support staff.

Laptop, Surface Pro and iPad users will not automatically have 'administrative rights' on their device and therefore may not be able to install programs or additional software on it.

When school devices have files that contain sensitive or confidential information, the user should password protect or encrypt them in case the laptop is stolen. Information about how to do this is available from the IT support staff.

Social media accounts connected with life and work at the School must be run in liaison with the Director of Marcomms. If pupils assist in the running of that account, the teacher in charge must see all output prior to publication and the pupils must only publish with permission from that teacher.

Prohibited Uses (not exclusive)

- Accessing Inappropriate Materials – all material on the Surface Pro, iPad or laptop must adhere to the Alleyn's School ICT Acceptable Use Policy. Users are not allowed to send, access, upload, download or distribute offensive, threatening, pornographic, obscene, or sexually explicit materials;
- Illegal Activities – Use of the School's internet/e-mail accounts for financial or commercial gain or for any illegal activity;
- Violating Copyrights;
- Cameras – Users must use good judgment when using the camera. The user agrees that the camera will not be used to take inappropriate, illicit or sexually explicit photographs or videos, nor will it be used to embarrass anyone in any way. Any use of camera in toilets or changing rooms, regardless of intent, will be treated as a serious violation;
- Images of other people may only be made without the permission of those in the photograph;
- Posting of images/movie on the Internet into a public forum is strictly forbidden, without the express permission of the Teacher or in the case of staff use; a member of the Senior Management Team;
- Use of the camera and microphone by pupils is strictly prohibited unless permission is granted by a teacher;
- Misuse of Passwords, Codes or other Unauthorised Access – users must set a passcode on their Surface Pro or laptop to prevent other users from accessing it;
- Malicious Use/Vandalism – Any attempt to destroy hardware, software or data will be subject to disciplinary action;
- Jailbreaking – jailbreaking is the process which removes any limitations placed on the Surface Pro or laptop by Apple. Jailbreaking results in a less secure device and is strictly prohibited;
- Gaining access to another user's accounts, files or data is strictly prohibited and anyone doing so will be subject to disciplinary action;
- Sharing use of the Surface Pro or laptop with pupils – there must be no time when a staff Surface Pro or laptop is given to a pupil for use, other than in a classroom/activity setting where the teacher is monitoring the use at all times for the benefit of the class/activity;
- Inappropriate media may not be used as a screensaver or background photo. Presence of pornographic materials, inappropriate language, alcohol, drug or gang related symbols or pictures will result in disciplinary actions.

Users Responsibilities

Users must use protective covers/cases for their school devices.

The Surface Pro, laptop and iPad screen is made of glass and therefore is subject to cracking and breaking if misused. Never drop nor place heavy objects (books, laptops, *etc.*) on top of your school device.

Only a soft cloth or approved laptop screen cleaning solution is to be used to clean the Surface Pro or laptop screen.

Do not subject the Surface Pro or laptop to extreme heat or cold.

Do not store or leave unattended in vehicles.

The School devices are subject to routine monitoring by Alleyn's School.

Users in breach of the Acceptable Use Policy may be subject to but not limited to; disciplinary action, confiscation, removal of content or referral to external agencies in the event of illegal activity. The Alleyn's School ICT Acceptable Use Policy for staff applies to the use of Surface Pro or laptop devices.

Alleyn's School is not responsible for the financial or other loss of any personal files that may be deleted from a Surface Pro or laptop. Local files on the Surface Pro or laptop can be backed up on the School network by use of One Drive.

I understand and agree to abide by the expectations of staff use of IT facilities, as stated in this AUP for Staff using IT Facilities - Section 1 or Sections 1&2 depending on what has been issued to me:

Name:

APPENDIX 4 – FILTERING AND MONITORING SYSTEMS (Section 11 of Appendix 4 of the Safeguarding and Child Protection Policy)

11. Online Safety

The DSL has responsibility for understanding the filtering and monitoring systems and processes in place.

The principles outlined in the School's IT and E-safety policy continue to apply. The IT support team will continue to ensure that appropriate filters and monitoring systems are in place to protect the School's IT systems.

Filtering and monitoring in the School is implemented in the following ways:

We use FortiGuard Web Filtering (FGWF) on the Firewall Gateway level to ensure a safer and more productive online environment for our users. FGWF is the highest-rated web filtering service in the industry for security effectiveness. It provides comprehensive threat protection to address threats including ransomware, credential-theft, phishing, and other web-borne attacks. It uses AI-driven behaviour analysis and correlation to block unknown malicious URLs almost immediately, with near-zero false negatives. FortiGuard URL Database is based upon the Web content viewing suitability. The categories for schools to block the access include but are not limited to: Academic Fraud, Adult/Mature Content, Alcohol, Dating, Gambling, Games, Lingerie and Swimsuit, Nudity and Risque, Other Adult Materials, Pornography.

We have also implemented the Impero Education Pro system to provide a further level of internet safety for our users with powerful, keyword detection tools to capture, record and identify early warning signs of harmful online behaviour. Its keyword library index contains thousands of keywords to identify students accessing harmful online content such as suicide, mental health, eating disorders, (cyber) bullying, or any other sensitive topic on their device.

When users are away from the School network (*eg* chatting on Microsoft Teams) we are covered by Senso Teams Chat Monitoring Safeguarding software. This is a cloud-based system and integrated with an AI based visual threat detection engine. Senso Teams Chat Safeguarding software will monitor chat and inspect images for visual threats and wellbeing, alerting the DSL when indicators are detected.

We use the Darktrace AI-powered cyber security solution, which is highly effective in preventing, detecting, and responding to unusual web activities. For instance, it is able to prevent pupils from accessing VPNs or anonymous proxy websites, installed on BYOD devices to circumvent the School's web filtering system.

We recently implemented Lightspeed web filtering solution (Lightspeed filter app) to help Junior School pupils manage and monitor internet usage on their iPads used outside of school network. This filter app is designed to enable content filtering and safe browsing on iOS devices by routing internet traffic through Lightspeed Systems' servers for analysis and filtering. The system also provides reporting and monitoring features that administrators can access insights into internet usage patterns, websites accessed, and potential policy violations. This information can help administrators ensure compliance with acceptable use policies and identify any safeguarding issues.

The DSL will hold an annual audit with the relevant members of the IT staff to audit the filtering and monitoring systems and their effectiveness.

At induction, staff will receive appropriate online safety guidance as part of their safeguarding and child protection training, including ensuring an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring.

The School will:

- identify and assign roles and responsibilities to manage filtering and monitoring systems
- review filtering and monitoring provision at least annually, with the input and awareness of a representative of the Governing Board
- block harmful and inappropriate content without unreasonably impacting teaching and learning
- have effective monitoring strategies in place that meet their safeguarding needs
- ensure that an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring should be included in safeguarding training
- ensure the Governing Board reviews the standards and discusses with IT staff and service providers what more needs to be done to support schools and colleges in meeting this standard.

The Governing Board, thus, will assist in reviewing standards and discussing with IT staff (and service providers) what more needs to be done to support the School in meeting the standard in line with the Prevent Duty.

Messages around online safety will continue to be a feature of our pastoral care via tutors and assemblies. The School has recommended to parents that they take reasonable steps to check that their child is staying safe online. The School has advised parents to check the privacy and security settings of home networks carefully. The School has asked that pupils report safeguarding incidents that occur online (such as harmful online content or cyberbullying) to us as soon as possible so that the School may follow them up, and pupils may report harmful online content via the UK Safer Internet Centre at <https://reportharmfulcontent.com>

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk the so-called '4Cs':

content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (*e.g.* consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and,

commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (<https://apwg.org/>).

Online teaching will follow the same principles as set out in the relevant staff code of practice/conduct and the School has published specific guidance on remote learning protocols and online safety for staff, including practices for live remote audio or video contact with individual pupils and live-streaming of audio and visual content (see separate appendix).

The School reminds pupils, parents and carers about the importance of safety online when away from the School, especially in accessing dangerous or inappropriate online sites. This is covered in the PSHE programme in regular reminders to children in different forums.

APPENDIX 5

The following Acceptable Use Agreements apply to pupils in the Junior School

EYFS Acceptable Use Agreement

Use Technology Safely



✓ I ask before I use a tablet, computer or camera.

✓ I tap or click on things I have been shown.

✓ I check if I can tap/click on things I haven't seen before.

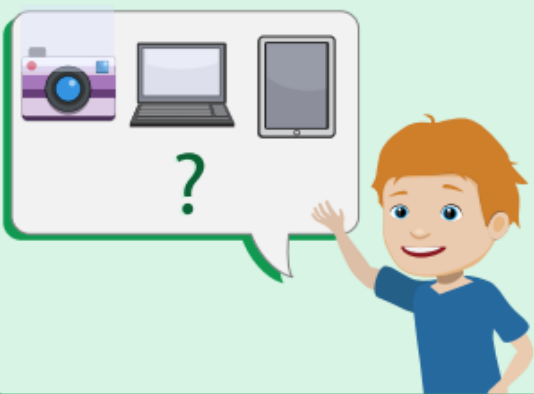
✓ I tell a grown-up if something upsets me.

My Name:

Class:

KS1 Acceptable Use Agreement


Use Technology Safely



✓ I ask before I use a tablet, computer or camera.



✓ I tap or click on things I have been shown.



✓ I check if I can tap/click on things I haven't seen before.



✓ I tell a grown-up if something upsets me.



I am kind and polite to others online and I only communicate with my friends and family.



I know that my personal information should never be shared online.

My Name:

My Class:

Today's Date:

Junior Acceptable Use Agreement

Use Technology Safely and Responsibly

I will only access computing equipment when a trusted adult has given me permission and is present.	I will respect computing equipment and will immediately notify an adult if I notice something isn't working correctly or is damaged.	I will only use the school's computers and iPads for set schoolwork and homework.
I will immediately inform an adult if I see something that worries me, or I know is inappropriate.	I understand that if I behave negatively whilst using technology towards other members of the school, my parents/carers will be informed, and appropriate actions taken.	I am fully responsible for the content of documents I create or upload, as well as any comments that I make on the Hub and MS Teams.
I will keep my username and passwords secure; this includes not sharing it with others.	I will only edit or delete my own files and not look at or change other people's files without permission.	I will not bring my personal devices into school, unless given permission.
I understand what personal information is and will never share my own or others' personal information such as phone numbers, home addresses and names.	The messages and comments I make on the Hub, Teams and online will always be polite, kind and sensible.	I must hand in my mobile phone to the school office when entering the premises and then collect it when leaving.
I am aware that some websites, games and social networks have age restrictions and I should respect this.	I am aware that my online activity in and out of school, should not upset or hurt other people and that I should not put myself at risk.	I will not change any settings on the computers or iPads, including the home screen.

I have read and understand these rules and agree to them:

Name:

Date: