Alleyn's School

Acceptable Use Agreement for Staff Using School IT Facilities

Policy Name	Acceptable Use Agreement for Staff Using School IT Facilities
ISSR	N/A
Reviewed by	SLT
Author/SLT	Mrs Mel Joel, Designated Safeguarding Lead
Date of school review	June 2024
Date of next school review	September 2025

Overview

Section 1 of this agreement applies to all staff. Section 2 of this agreement 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 and mobile device (school or personally-owned) usage.

It is subject to the *Acceptable Use Agreement* 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 IT and E-safety 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 Agreement* 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 and Child Protection 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 Safeguarding and Child Protection 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 into that communication.

Members of staff must pay due regard to the School's guidelines on use of photography and video, as outlined in the Safeguarding and Child Protection 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 Alleyn'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 fileservers. 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 Head of IT Services and Systems.

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 and Child Protection Policy and code of practice for staff should be followed when dealing with these kinds of incidents. The School's IT Support 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 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 External Relations and the Marketing and Communications Team. 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 or laptop must adhere to the Alleyn's School IT Acceptable Use Agreement. 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 with 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 Agreement 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.

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 AUA for Staff using IT Facilities - Section 1 or Sections 1&2 depending on what has been issued to me:

Name: ....

Signed: .... **Date:** ....