Every child a scholar

Arts & Media School

ISLINGTON

# Draft IT Acceptable Use Policy

# 2022-2023

This policy document relates to the use of ICT and is a guide to staff to ensure safe use, safeguarding themselves, the school and the children. The use of ICT and social media communications are vital tools in effective school organisation and communication practices. All staff are required to be highly responsible in its use. Staff should be aware that misuse can have very serious implications for individuals and the reputation of the school.

Staff need to be aware of the risks any misuse of IT can present. Things done purposefully or as consequences of lack of awareness or naivety can result in difficulty. There is a professional responsibility expected of all staff to keep abreast of developments and to use IT applications at all times maintaining a professional persona. Staff are expected to strictly act in accordance with the responsibilities of a staff member, and role model, working in a school and ensure that IT use and ICT communications are entirely appropriate. All IT use is expected to be appropriate, including that which is personal (on personal IT accounts) as well as school business (amsi.school and school accounts). Inappropriate use can reflect back on individuals in their professional life as an employee at the school; this is the nature of the network and social media. These include for instance, comments on Twitter, photos posted on Facebook, emails, WhatsApp communications or items retrieved from the internet.

**Responsibility.**

All staff members are expected to strictly adhere to this policy, which will be periodically updated and available to all staff on the Staff Shared Drive. Where it is believed that an employee contravenes this policy, the School/Islington Disciplinary Procedures would be applied as might be appropriate.

**Internet Access**

The School provides Internet access for research and educational use. The content of sites visited is monitored and filtered. AMSI has its own procedures to monitor (Smoothwall) and filter sites which are supported by LGfL. Common sense is urged when using the Internet. The School operates both a proxy server and a firewall. This may result in some applications being unable to access the Internet. To maintain the security of the network, do not attempt to circumnavigate or knowingly bypass the internet filter.

**Safe use of the internet**

- Remember that the internet is public access – consider how information posted by you could affect your image and the image of the school.
- Periodically check the information which is available about you on the internet.
- Use a range of passwords for different websites (passwords should include letters, characters and numbers).

**E-mail**

Email use is encouraged where this supports the goals and objectives of the school. However, staff using AMSI email must ensure that they:

- comply with current legislation
- use email as a professional communication
- do not create unnecessary risk to the school, children or staff by misuse
- Be aware that email may be forwarded without their knowledge.
- Ensure that communications going outside of the school represent the school

The use of email is a valuable communication tool. Nevertheless, misuse(s) of this facility can potentially have a negative impact upon staff morale, corrupt the school system or damage the reputation of the school/individual.  Special care should be taken to avoid such misuse.

The school's email resources are provided for school related communication purposes.
E-mails should not, as a matter of course, be regarded as private and any e-mail sent through the School domain remains the property of the School.
The Laws regarding the use of electronic mail are fairly stringent. Certain offenses regarding libel and publication of obscene material also apply to items transmitted through e-mail.
Therefore, in order to protect pupils and staff the school maintains the right to examine any systems and inspect any data recorded in those systems including school email accounts.

**Examples of unacceptable ICT practice**

- forwarding of school confidential messages to external locations
- distributing, disseminating or storing images, text or materials that might be considered indecent, pornographic, obscene or illegal
- distributing, disseminating or storing images, text or materials that might be considered discriminatory, offensive or abusive, in that the context is a personal attack, sexist or racist, or might be considered as harassment
- accessing copyrighted information in a way that violates the copyright
- breaking into the school's or another organisation's system or unauthorised use of a password/mailbox
- broadcasting unsolicited personal views on social, political, religious or other non-school related matters
- transmitting unsolicited commercial or advertising material
- undertaking deliberate activities that waste staff effort or networked resources
- introducing any form of computer virus or malware into the school network
- use of school communications systems to set up personal businesses or send chain letters

**Mobile Devices**

Mobile technology offers huge opportunities for both staff and pupils. AMSI is keen to exploit the possibilities associated with these developments whilst protecting the individual security of staff and the reputation of the school. Many of our pupils are digitally literate and this could raise issues for less digitally literate staff.

This **guidance** is designed to protect and support staff and children.

- Add a passcode to your phone so that it cannot be accessed by anyone else if you lose it.
- If you choose to phone parents from your mobile, remember to withhold your number (141 before you dial). The school system does this automatically.
- Do not give your phone number to pupils.

**Portable storage e.g. USB etc**

It is preferred that data is stored on your Google Drive or on your network drive through remote access. Where this is not possible, please follow the guidelines below:

- Ensure that all data stored portably complies with the GDPR regulations.
- When transporting confidential information, ensure that this information is secure e.g. lock up storage devices and delete confidential information after use.
- Consider using email attachments for confidential information as they are password protected.
- Ensure all work on USB is backed up elsewhere to prevent the loss of your work.
- Remove USB safely using the icon at the bottom of your desktop.

**Networked Computers**

The use of computers in school is intended for educational purposes. All desktop computers connected to the network are the property of the School. No cables, peripherals or other hardware should be removed from or added to the desktop computers without prior instruction by the network manager or business manager.

No software should be installed on any desktop hard-drive without prior permission from the network manager or IT manager. Any unauthorized software will be removed. You must give up use of any desktop computer required by the network manager or IT manager for the purposes of maintenance.

Staff must only use school equipment for the purpose for which it was designed. You may be liable for any damage caused.

**School Network and personal laptops and other IT devices**

All staff are to refrain from plugging their own personal devices into the school network unless you have obtained permission from either the network manager or IT manager. This is to avoid introducing viruses and malware or any other network breaches

### Remote Network Access

If you have been granted remote access to the school network, ensure that the computer or laptop you are using is not left unoccupied. If you need to be away from your computer please log out of the session. Accessing the school network remotely from a public computer (i.e. internet café) should be avoided.

### Software

Relevant software is approved and provided by the ICT Team, as and when it becomes available. The addition of other software to the desktop computers and/or the network is only allowed after agreement by the network manager or IT manager. Any requests for new software must be made to the ICT Team.

Users (subject areas) are responsible for the purchase of any licenses that may be required by software by that curriculum area. The school will not install or provide any software that is unlicensed, and will not knowingly consent to any activity that would infringe on current licensing laws. Please seek the advice of the network manager or IT manager if you are unsure about software requirements or licensing.

### Viruses

Any user who knowingly installs or transmits a virus through the school network will be dealt with using the appropriate Personnel Procedures. Viruses should not be transmitted through the e-mail system or transported on USB flash drives. Any e-mail or other medium that is found to have a virus installed will be physically destroyed.

### School Chromebooks/Laptops

All chromebooks/laptops remain the property of the school. Chromebooks/Laptops can be prone to malfunction and damage. All chromebooks/laptops must have valid and current anti-virus software installed and updated. Third-party laptop owners are responsible for providing and maintaining their own anti-virus solution. Do not connect your personal laptop to the school network without prior permission from the network manager or IT manager.

Chromebooks/Laptops may be required for audit at any time to check for general condition. Chromebooks/Laptops must be well maintained, if chromebooks/laptops are to be used at home you should acquire suitable insurance cover. All chromebooks/laptops must be kept in a safe place when not in use.

All staff are required to adhere to GDPR regulations, therefore, school data should not be stored on personal devices, laptops, smartphones etc.

Students it is your responsibility to ensure the chromebooks are returned in good condition at the end of your stay at AMSI.

## Network Accounts

You must only use the account set up for you. Any account that is suspected of being used by more than one user will be suspended. You should not reveal your password, and do not allow others access to your account. The Shared Drive storage and user account use will be monitored and audited, both for usage habits (hours of use and length of time) and content in order to increase the efficiency of the Network.

All user accounts are regarded as private, although they and any material within them are the property of the school. They may be inspected or altered in the course of routine maintenance. The same applies to e-mails sent through the school network.

Any pupil or staff member caught or suspected of ‘hacking’ or attempting to ‘hack’ the network in any way will be subject to disciplinary procedures. The definition of 'hacking' for the purpose of this document is "any unauthorised access to any file or resource, whether damage is caused or not". It must be pointed out that the provision of a network account is a benefit that may be withdrawn for misuse.

**By its nature, this guidance can quickly become out-of-date, please inform the IT manager and the Safeguarding Team if you hear of new issues that we need to consider.**

## Remote Learning (Link to Remote Learning Policy)

Arts and Media School is committed to providing learners with home learning materials alongside their class stationery pack (this might need to be delivered). In the case of whole cohort isolation, resources will be available on one of the online learning platforms and priority learners will have packs delivered. This measure will afford teachers a short time to prepare and set up their remote learning resources that will be delivered via Google Classroom or Google Meets.

# STAFF IT ACCEPTABLE USE AGREEMENT

This policy outlines rules intended to protect both our IT network and our school community. It is a requirement that all staff who use school IT equipment are expected to comply with and agree to this policy.

------------------------------------------------------------------------------------------------------------------

**When any staff member logs onto the school network or school domain, and chooses to use it, they thereby confirm agreement to abiding by these acceptable use requirements.**

**This is set up as an initial requirement when staff first attempt to log-on to use the school network and email system.**

------------------------------------------------------------------------------------------------------------------

The network and internet use

1. I will use the network and the internet responsibly and I understand that the school maintains the right to monitor my use of the internet.
2. I will keep my logins, IDs and passwords secret.
3. I will take care when bringing electronic files into school (on removable media or online) to ensure network security and I will not download and install software without permission.
4. I will not try to hack into the network or bypass its security features.
5. I will only edit or delete my own files and not view, or change, other people's files without their permission.

Confidential data and SIMS

1. I will log off from SIMS whenever I am not using it.
2. I will lock my computer, if SIMS is open, when I leave my desk (using CTRL + ALT + DEL and spacebar key combination).
3. I will follow the Remote Learning Policy/Protocols
4. I will take care to protect any sensitive data which may put staff, pupils or others at risk.
5. I will regularly change my SIMS password.
6. I will make sure personal data printed from SIMS is stored securely.
7. I will make sure personal data from SIMS or any other document is not projected on the whiteboard.
8. I will not allow pupils to access SIMS under any circumstances. This includes not letting pupils take a register once I have logged on.
9. I will not store personal data on pupils on unsecured portable media devices like USB sticks or transmit personal data on pupils from a non-AMSI email address.

Note that in cases where it is believed that an employee contravenes this policy, and if considered appropriate, disciplinary procedures could be applied.

## IT Acceptable Use Policy

It is your responsibility to ensure that you have read this policy and understand clearly the contents of this policy.

The use of Arts and Media School ICT resources and services is a facility granted, at the school's discretion, to pupils. This AUP is essential for managing and sustaining the integrity and legality of the Arts and Media School network and computing resources.

### General

- Use of the Arts and Media School school network constitutes agreement to comply with this policy.
- These rules apply to the use of any of the school computers, wherever they may be. They also apply whenever a user is logged on to the Arts and Media School network or domain.
- Pupils are given a user account to enable them to use the facilities on the school network or domain, use of this account is monitored – it is neither private nor privileged.
- Pupils are given an email account to use, the account is monitored and filtered, the user is responsible for the content on their account and is permitted to follow the generally accepted rule of network etiquette. These include but are not limited to: a. Users are not allowed to reveal their date of birth, personal address or contact number, nor the date of birth, personal address or contact number of other users. b. Users are not allowed to distribute images of themselves or others c. Users should be polite and use appropriate language. Do not swear or use vulgarities. Do not harass or bully.
- I will follow the Remote Learning Protocols.
- You must not use someone else's username to gain access to the school network or online account.
- You may not attempt to circumvent security of any host, network or account, or penetrate security measures (“hacking”) on or accessed through the Arts and Media School network.
- You must not use the network or your own property to access or process pornographic material, inappropriate text files, or files dangerous to the integrity of the network.
- You must not transmit, re-transmit, publish or store material on or through the Arts and Media School network which is bullying, threatening, abusive, hateful, indecent, or defamatory.
- You must report any unpleasant material or message sent to you. This report would help protect other pupils and you.
- If a pupil or user account breaches the above rules, their account may be inspected and their access disabled. They may also render themselves liable to sanction from the Headteacher up to and including suspension and exclusion.
- **Not to damage or deface the school ICT equipment in any way. This includes computers, keyboards, mice and any other equipment. Parents/Carers will be charged for any damages or repairs to equipment and Chromebooks.**

- **Chromebooks MUST be brought to school everyday fully charged. Students without a Chromebook will be sanction appropriately**
- Follow the Remote Learning policy required to do so.
- Above all, you should be **KIND AND SAFE ONLINE**.

Signed:

Student Name :_______________________________________________

Student Signature :_______________________________________________

Parent/Carer Name: _______________________________________________

Parent signature :_______________________________________________