Aysgarth School

Acceptable Usage Policy for Staff

Reviewed: September 2023 and to be reviewed October 2024
Responsible Member of Staff: Jo MacLelland

Aysgarth ICT Acceptable Usage Policy for Staff

(reviewed September 2023)

This is the Acceptable Usage Policy (AUP) for Staff at Aysgarth School. The purpose of this policy is to promote positive and responsible network and internet behaviour. Please read carefully and sign at the bottom to show you agree to these terms. If you do not sign and return this form you will not be able to use the school's IT systems.

The use of the latest technology is actively encouraged at Aysgarth School. With this comes a responsibility to protect users and the school from abuse of the system.

All staff, therefore, must adhere to the policy set out below. This policy covers all computers, laptops, phones and electronic devices (such as iPod touches and iPads) within the school, irrespective of who owns the device.

Staff and pupils are expected to behave responsibly on the school computer network and with the ICT equipment.

As a staff member at Aysgarth School, I may have access to the following ICT facilities:

1. My own school laptop and computers in the IT lab.
2. Smartboards or projectors & displays in classrooms.
3. A docking station and speakers in classrooms.
4. A secure username and password for logging into school computer systems.
5. An accredited, filtered Internet connection from any computer in school or wifi connected device.
6. Personal (Google Drive) user space with unlimited storage for my emails and documents.
7. Internal and external remote access to the school network and Google Drive to store and share learning resources and other school related documents.
8. A personal @aysgarthschool.co.uk email account with unlimited email storage space.
9. Access to network printers and copiers. Usage is monitored by Papercut software.
10. Access to school mobile phones, flip video recorders, scanners, digital cameras, iPads and microphones.
11. Access to the following software for use on my laptop:
    a. The Google Apps suite
    b. Smart Notebook 11
    c. Sophos Antivirus
    d. Microsoft Office
    e. Access to the School Management Information Systems (SchoolBase) as appropriate to my role in school at school and from home.
12. If I bring in my own ICT equipment I can see ICT support personnel to connect it to the school wireless staff network.

E-safety

1. I will ensure that I am aware of e-safety issues affecting staff and pupils.
2. I will regularly remind pupils of key e-safety messages such as 'never give out personal details online'.
3. I will report any accidental access to inappropriate material to my line manager.
4. I will be vigilant when asking pupils to search for images.
5. If a pupil accesses inappropriate material I will report it to a member of the Senior Management Team.
6. If I suspect a child protection issue, (including grooming, pornography and radicalisation) I will report it following the correct procedures.
7. I will always be myself and will not pretend to be anyone or anything that I am not on the internet.

Computer Security

1. I will use computers with care and leave ICT equipment as I found it. I will not tamper with computer systems or devices (eg printers and projectors) and their cabling.
2. If I notice that ICT equipment or software is damaged or not working correctly, I will report it to the ICT department.
3. I will never try to bypass security features or systems in place on the network, or try to access resources or a user account that I do not have permission for (hacking).
4. I will never attempt to install software on school computers or mobile devices myself (unless I have the ICT Manager's permission) and will request a software change through the ICT department.
5. I will always keep my user account credentials secure and not tell them to anyone else.
6. I understand that my staff logon gives me access to systems and information that pupils and other staff are not entitled to access and I will not under any circumstances allow anyone else access to a computer under my logon credentials
7. I will not attempt to go beyond my authorised access. This includes attempting to log on as another person, sending emails whilst pretending to be another person or accessing another person's files. If I find that I do have access to an area that I know I should not have access to, I will inform ICT support personnel immediately.
8. If I think someone else has obtained my login details, I will report it to the ICT department as soon as possible to get my logon credentials changed.
9. I will never knowingly bring a computer virus, spyware or malware into school.
10. If I suspect a school computer or a removable storage device that I am using contains a virus, spyware or other malware, I will report this to the IT department.
11. I will not attempt to connect to another user's laptop or device while at school. I am not permitted to establish my own computer network.
12. I will take care if I eat or drink whilst using ICT equipment.
13. I will not reply to spam emails as this will result in more spam. Delete all spam emails.
14. If I lose or misplace any portable ICT equipment I will inform ICT support personnel immediately.

15. I will not 'jailbreak' a school iPad by installing a different operating system.

Inappropriate Behaviour

1. I will not use a mobile phone in the vicinity of EYFS setting or children.
2. I will not store, download or distribute music, video or image files on my personal user space or shared area, unless they are appropriately licensed.
3. I will not send or post defamatory or malicious information about a person or about school.
4. I will not post or send private information about another person.
5. I understand that bullying, manipulation or exploitation of another person either by email, online or via text message will be treated with the highest severity.
6. I will not access material that is profane or obscene, or that encourages illegal acts, violence or discrimination towards other people.
7. If I am planning any activity which might risk breaking the ICT Acceptable Use Policy (eg research into terrorism for a legitimate project), I will inform the ICT department beforehand to gain permission.
8. If I mistakenly access material that is profane or obscene, I will inform my line manager immediately or I may be held responsible.
9. I will not attempt to use proxy sites on the internet.
10. I will not take a photo or video of a pupil using a personal device. I will only use a school device to take photos or videos.
11. I will not take a photo or video of a pupil or another member of staff, using a school device, without their permission.
12. I will not load photos or videos of other staff and pupils to websites or social networking sites. I will refer this job to the Boarding Team, IT department or Marketing department, unless I am given permission by the Headmaster. (eg if I wish to put pictures from a trip on the school website).
13. I will not store photos or videos, unless they have been used for public use e.g. twitter or school website, of pupils and staff on personal cameras, phones, home computers or other devices.

Monitoring

1. I understand that all Internet and email usage will be logged and this information could be made available to my manager on request.
2. I understand that all files and emails on the system are the property of the school. As such, system administrators have the right to access them if required.
3. I will not assume that any email sent on the internet is secure.
4. I understand that all network access, web browsing and emails on the school systems and laptops are logged and may be routinely monitored on any computer screen without the person's knowledge.
5. I am aware that all internet access is filtered by the school using a Fortigate firewall.
6. I understand that if the filter systems fail and allows access to a possibly inappriopriate

site that I will report this to my line manager and ICT Manager.

Best Practice

1. I will switch personal devices to silent whilst on the school premises. I will only use a personal mobile phone away from the view of the pupils.
2. When in charge of pupils I will only use a school mobile device, unless there is an emergency (with the exception of the trips policy instructions)
3. When conducting a remote lesson, using Google Meet, I will record the lesson so that it can be accessed at a later date, if required.
4. I will not use school printing facilities to print non-work related materials without authorisation, and agreement of costs, from the Bursar.
5. I will only print out work that I need as a paper copy – where possible I will use school systems such as email, the Google Drive and shared folders to share information electronically.
6. I will report it to the ICT department if I believe a printer is not working or out of toner.
7. I understand that my @aysgarthschool.co.uk email is a work email account, and as such I will use it predominantly for professional purposes.
8. I will only use the approved, secure @aysgarthschool.co.uk email system for any school communication.
9. I will only open attachments or download files from trusted sources.
10. I will not view, download or distribute material that could be considered offensive, pornographic or promote radicalisation.
11. I will save work regularly using sensible folder and file names.
12. I will organise my files in a sensible manner and tidy my user space and shared resource areas regularly.
13. I will observe health and safety guidelines where possible when using ICT equipment.
14. I will leave my computer and the surrounding area clean and tidy.
15. When I leave school permanently, I will ensure that I save any files I wish to take with me as my account will be deleted. I understand that confidential school files should be deleted from my account.
16. When I leave school permanently, I will ensure that any files I have stored on mobile or external devices and are needed by school are moved back on to the school system.
17. I will seek advice from the ICT department before ordering any ICT equipment for my department.

Data Protection

1. I will not share data protected information (including school images) with third party organisations without seeking advice first.
2. I will not use a storage device (such as a USB drive, encrypted or not) to transfer data protected files between home and school. Alternatively, I will either use Google Drive or remote access to move the files.
3. I will ensure that I am aware of data protection issues and understand what is considered

to be ‘personal data’.

4. I will not display sensitive information or ‘personal data’ on a public display or projected image (eg a smartboard). This includes pupil data in SchoolBase.
5. I will not leave a computer logged on and unattended for even a short space of time. I will log off or lock the workstation. I understand that failure to do this may result in a breach of the Data Protection Act and leave ‘personal data’ unprotected.
6. I will ensure that any remote connection session that I have to a school computer is logged off when I have finished and kept secure from other computer users.
7. I will ensure that my laptop is secure at all times when taken off site.

Social Networking

1. I will not communicate with pupils through social networking sites. I will deny current or past pupils (until the age of 19) access to my profile so they do not put me in a vulnerable position.
2. I will ensure that my privacy settings for any personal social networking account are set to be secure, allowing minimal access to my information - e.g. Facebook privacy and timeline settings should allow access for “friends” and not “friends of friends”.
3. I will never create a social networking profile, blog or account and use it for school purposes without prior written authorisation from the Headmaster.
4. If I have control over a school Twitter account I will
    a. keep it as a protected account at all times.
    b. not follow individuals or organisations or allow to be followed.
    c. inform ICT department straight away if I suspect I have lost the password or a device with that account on it
    d. never use the account to send Direct Messages to anyone.
5. I will never create a bogus social networking account or site that is associated with a member of staff, pupils or the school.
6. If I become aware of misuse of Social Networking accounts or sites that are associated with a member of staff, pupils or the school, I will inform the IT department immediately.
7. I recognise that as an organisation, we do not use social networking sites to communicate with pupils, staff and parents (with the exception of our official Twitter and Facebook accounts).

Sanctions

1. I understand that failure to comply with this Policy could lead to disciplinary action.

Signed: _____

Date: _____