



TARLETON
ACADEMY

FACIMUS NOSTRAE FUTURAE

Acceptable Use Policy

June 2018

Acceptable Use Policy

Purpose

The document defines the Academy's policy to ensure that all users of technology within school are responsible and are protected from potential risk in their everyday use of Information Communications Technology (ICT) for educational, personal and recreational purposes. This Acceptable Use Policy (AUP) and the signed Network Use Permission Form is an agreement between parents, students, staff, governors and the Academy to ensure that users are kept safe when using technology.

Statement of Principle

This policy reflects the Academy's commitment to providing a diverse, balanced and relevant approach to the use of technology and is directly linked to the Academy's strategic aims ([Vision, Motto and Strategic Aims](#));

- Outstanding education at the heart of the community
- Every individual becoming the best that they can be
- Consistently high quality teaching which places the learning of the individual at the heart of everything
- A total commitment to a caring environment, where everyone feels safe and valued
- Support and challenge through inspirational and engaging leadership

Scope

This policy outlines the commitment of all staff, students, parents and governors to ensure that all users in the school environment are,

- encouraged to maximise the benefits and opportunities that technology has to offer
- work in an environment where security measures are balanced appropriately with the need to learn effectively
- equipped with the skills and knowledge to use technology appropriately and responsibly
- able to recognise the risks associated with technology and how to deal with them, both within and outside the school environment
- understand why there is a need for an AUP

Users of the Academy technology may include

:

- Students,
- Staff,
- Parents,
- Governors,
- Visitors,
- Multi-agency staff linked to the Academy,
- Trainees on placement.

Acceptable Use Policy

Background

Electronic information research skills are now fundamental to all aspects of school life. Staff will investigate possibilities and blend use of such information as appropriate within the curriculum and will provide guidance and instruction to students in the appropriate use of such resources.

Staff will consult with the Senior Leadership Team (SLT) for advice on content, training and appropriate teaching levels consistent with the Academy programme of study. SLT will ensure that appropriate procedures are in place for implementing this policy and for reviewing and evaluating its effect on teaching and learning.

Impero has been implemented within the Academy and allows the Academy to monitor and enforce this AUP. This software analyses, manages and reports inappropriate traffic flowing to or from the Academy network.

Privacy

In particular please note the provisions set out in this policy about privacy and how the Academy may monitor data, information and material in relation to or used, sent or received by you.

The Academy will try to respect your privacy but in order to protect pupils' safety and well-being and to protect the Academy from any third party claims or legal action against it, the Academy may view any data, information or material on the Academy's ICT system (whether contained in an e-mail, on the network, notebooks or laptops) and in certain circumstances, disclose that data, information or material to third parties, such as the police or social services. You consent to the Academy viewing, using and disclosing data, information or material in relation to, used, sent or received by you.

The Academy disclaimer at the end of our e-mails notifies the recipient that any e-mail correspondence between you may be monitored. You must not remove this disclaimer.

Network Access and Email

Access to the Academy network, the Internet, email, the Virtual Learning Environment (VLE), Cloud based data storage and Chromebook usage will be provided, but only on the understanding that users agree to follow these guidelines. These guidelines apply to all computer users.

Computer (file) storage areas will be treated as school property. Senior staff may look at files and communications to ensure that the system is being used responsibly. Users should not expect that their work and emails would always be private. You should also be aware that a member of staff can view your computer screen at anytime from anywhere on the school network without you knowing about it.

Acceptable Use Policy

Email

All users have access to the Lancashire Grid for learning service as the preferred school email system. Non-approved email accounts must not be used for any Academy business and only official email addresses (@tarletonacademy.org) should be used to contact students, parents, staff, governors, trainee teachers and external business contacts.

Any electronic contact with students should be made only through the Academy's Firefly or email account.

E-mails constitute records of the Academy and are subject to the same rules, care and checks as other written communications sent by the Academy so, for example:

- You should always consider whether it is appropriate for material to be sent to third parties;
- they may have to be disclosed in legal proceedings;
- they may have to be disclosed to a person if he makes a request to see information held about him under data protection law;
- they require the same level of authorisation before being sent;
- printed copies of e-mails need to be retained in the same way as other correspondence;
- they are confidential to the sender and recipient, unless you have been given permission to read them;
- transmitting the works of others, without their permission, may infringe copyright;
- sending or storing messages or attachments containing statements which could be construed as improper, abusive, harassing the recipient, libelous, malicious, threatening or contravening discrimination legislation or detrimental to the is a disciplinary offence and may also be a legal offence.

You must ensure that confidential emails are suitably protected at all times.

Instructions for All Computer Users in School

- Users are responsible for good behaviour on the computers just as they are in a classroom or a school corridor. General school rules apply.
- Users should be aware that all their username and passwords should be kept safe and not disclosed at any time to any other person.
- Users are fully responsible and accountable for anything that happens whilst they are logged on to a computer. Users should not under any circumstances leave a machine unattended whilst it is logged on, unless it has been locked by the user, as any resulting misdemeanour is accountable to the logged on user.
- Do not use another person's user account, use only your own username and password. Shared work should be emailed to your working partner.

Acceptable Use Policy

- Do not reveal your password to anyone. If you think someone knows your password then change it immediately, or request for it to be changed.
- The unauthorised access or use of personal information is not permitted.
- Eating, drinking, personal grooming, and the use of aerosol sprays are not considered to be suitable activities in any classroom. In a computer room they may cause serious damage and are strictly prohibited.
- Be considerate to other users as they may be waiting to use the computer.
- It is your responsibility to save important work files to the appropriate storage area.
- Any data stored may be deleted or utilised in the needs of the Academy once you have left the Academy.
- If a "virus alert" occurs please inform a member of the teaching staff or the IT Technician immediately.
- Intentional damage to computers, computer systems or computer networks, including unauthorised damage or interference to any files is not permitted and the cost of the damage may be recovered.
- Programs must not be installed on a computer except by the IT Technician. Do not bring in programs on a pen drive or DVD or download them from the Internet.
- Games must not be loaded, played or used on any computer unless used for authorised training or teaching purposes.
- Music and Video files must not be downloaded unless you have permission to do so.
- The unauthorised copying of software is not permitted.
- The installing, copying or transmitting of obscene material is not permitted.
- Always make sure that you have completely logged off the computer before leaving it unattended. If you are leaving the computer for a short while, e.g. to pick up a print out, you must lock the computer.
- Please leave the computer and the surroundings as you find them.

Acceptable Use Policy

Guest Network Access

Access to the network via personal devices is authorised and managed by the IT Technician.

Internet Use

Internet access will be provided to users to conduct research and communicate with others, but only on the understanding that users agree to follow these guidelines. These guidelines apply to all users of the Academy's computer systems both on and off the school premises.

General

- Users are responsible for good behaviour on the Network and the Internet just as they are in a classroom or a school corridor. General school rules apply.
- The Network and the Internet is provided for users to conduct genuine research and communicate with others. All the sites you visit are recorded. Remember that access is a privilege, not a right and that access requires responsibility at all times.
- The internet access system used by the Academy maintains a record which identifies who uses the facilities and the use that you make of them. The information collected includes which website and services you visit, how long you remain there and which material you view. This information will be analysed and retained, and it may be used in disciplinary and legal proceedings.
- You should be aware that a member of staff can view your computer screen at anytime from anywhere on the school network without your knowledge.

During lessons, staff will guide students toward appropriate materials. Outside of lessons, parents bear responsibility for such guidance, as they must also exercise with information sources such as television, telephone, cinema, radio, newspaper, magazine and other potentially offensive media.

The following are not permitted:

- Sending, displaying, accessing or attempting to access any obscene or offensive material including images of a pornographic corrupt or sexual nature.
- Using obscene or offensive language. Remember that you are a representative of the Academy on a global public system - never swear, use vulgarities, or any other inappropriate language. Bad spelling is also a poor reflection on you and the Academy.
- Harassing, insulting or attacking others through electronic media. Threatening with physical violence or mental torture and cruelty.
- Violating copyright laws. Never copy and make use of any material without giving credit to the author. By itself such work will be of little value as your own work. You should

Acceptable Use Policy

assume that all material on the internet is protected by copyright and must be treated appropriately and in accordance with the owner's rights. You must not copy, download or plagiarise material on the internet unless the owner of the website expressly permits you to do so.

- Revealing any personal information, the home address or personal phone numbers of yourself or other people.
- Downloading games or other executable programs. Downloading unlicensed music or video content.
- Use of commercial activities by for-profit institutions.
- Carrying on a private business.
- Undertaking financial transactions unless authorised to do so.
- Open unidentified email attachments.

Sanctions

1. Disciplinary action may result in line with the existing Academy Rewards and Behaviour Policy on inappropriate language or behaviour.
2. Violations of the Acceptable Use Policy may result in a temporary or permanent ban on your use of the school network.
3. When applicable, police or local authorities may be involved.

Social Networking and Other Forms of Social Media

Students are not permitted to access any social networking or social media websites while on the school premises.

All members of staff should refer to the Guidance on the Use of Social Networking Sites and Other Forms of Social Media policy which is available on Firefly.

Acceptable Use Policy

Password Security

All computer network access passwords must comply with the Academy Password Policy. System securities will enforce the necessary standards for passwords and regular password changes.

Network User Access

- Access to the school network is available from any network station during the normal school day. The IT Technician ensures that the stations in the classrooms and work areas are turned off at the end of the day (the system is automated). Prior arrangements must be made for access during school holidays.
- All users are required to log on with their own personal username, which will remain with them throughout their time at the Academy.
- All users have their own password to allow them to log on, which should not be made available to anyone else.
- Time spent on the network by each user is continually audited.

File Security

- All users have their own area for storing their work on the network server hard disk (the 'My Documents' folder). This means that they can access their work from any network station.
- To reduce the chances of the server hard disk filling up please do not save any unnecessary files in your 'My Documents' folders e.g. programs, pictures video and music.
- Users do not have access to local station and network system drives nor are they able to alter or save files outside their own area (except in the authorised shared areas) and must not attempt to access these areas.
- Precautions are taken to reduce the chances of infection by computer viruses via the Internet, email, pen drive, CD and DVD. The anti-virus software, which is installed on all school network stations and servers, is updated every day.
- Network stations must not be booted up from any external media, for example a Pen Drive.
- A regular search is made for any executable programs, unlicensed music and video stored in user areas. These are automatically logged against the user for subsequent action and then deleted.
- The system performs an automatic backup of each server hard disk to tape every night. A different tape is used for each night and then reused one week later. Regular backup tapes are also taken at key points (end-of-week, end-of-term, pre-upgrades, etc) and are kept for longer periods of time before reuse.

Acceptable Use Policy

- Station backups are not required. A faulty station can be quickly rebuilt with all the necessary software via files stored centrally on the server.

School Network Security

The school network is a valuable resource that is freely available to all students and staff from the majority of computers situated throughout the Academy. Precautions have been put in place to ensure that the system is available and in full working order.

This policy also reflects the Academy's Privacy Notice for Students and the Academy's Privacy Notice for the Workforce which are available on the Academy website.

Supervision

The use of the network should be supervised as closely as is reasonably possible during timetabled lessons. It should be realised however, that all users do have access to the network at other times and with very little supervision beyond the restrictions outlined below. Staff can view a computer screen at anytime from anywhere on the school network without the user knowing about it.

The Academy's computer network is equipped with a program that is able to detect inappropriate behaviour on the computer system. Violations of this AUP are recorded on a database and warnings are triggered when an incident occurs. The use of swear words and derogatory slang will result in the user having sanctions imposed.

- Access to many, if not most sites considered to contain "unsuitable" material is prevented by a filtering system used by our Internet Service Provider (ISP). As new sites of this nature come online and come to the attention of staff all over the country, they are filtered as soon as the service provider is notified.
- Access is prevented to "hacking" sites, executable files and many adverts.
- Access to Chat Rooms are filtered by our ISP.
- Precautions are taken to reduce the chances of infection by computer viruses via the Internet or email.
- Users found actively searching for "unsuitable" material or sending offensive email messages will have their access to the Internet denied and further action may be taken depending on the nature of the offence. Repeated abuse of the facilities will result in further and more serious action being taken.
- Users are not to alter the web level filtering on Internet search engines, e.g. 'safe search enabled' on Google.

Acceptable Use Policy

Mobile Devices, Tablet and Mobile Phone Use (including Bring Your Own Device, BYOD)

Students are not allowed to use unauthorised mobile devices and headphones on the school site. Any student seen with unauthorised mobile devices or headphones (including mobile phones, iPods, tablets, MP3 players) will have the item confiscated without any prior warning. To ensure that we operate in a fair and consistent way the Academy takes a zero tolerance approach to this principle. Behaviour systems and procedures are in place for any student who does not comply with this policy.

Any member of staff or visitors to school are required to have security settings enabled on their devices e.g. access passwords as per the BYOD policy. Users must ensure that all content on these devices is legal and appropriate for a school setting and should be aware that the school cannot be held liable for any damage or theft of personal devices.

Academy mobile phones are available for staff to use whilst outside of school and on authorised trips.

Students are not permitted to reconfigure their devices to attempt to bypass the Academy's internet safety systems.

DOCUMENT APPROVAL	
Mr M Cunniffe	Head of School
Approval Date:	June 2018