

TARLETON ACADEMY

Acceptable Use Policy

Network Access

The school encourages use of the rich information resources available on the network and Internet, together with the development of appropriate skills to analyse and evaluate such resources. These skills will be fundamental in the society which our students are entering.

On-line services significantly alter the information landscape for schools by opening classrooms to a broader array of resources. In the past, teaching and library materials could usually be carefully chosen. All such materials would be chosen to be consistent with national policies, supporting and enriching the curriculum while taking into account the varied teaching needs, learning styles, abilities and developmental levels of the students. Internet access, because it may lead to any publicly available site in the world, will open classrooms to electronic information resources which have not been selected by staff as appropriate for use by students.

Electronic information research skills are now fundamental to preparation of citizens and future employees during the current Information age. The school expects that staff will investigate possibilities and blend use of such information as appropriate within the curriculum and that staff will provide guidance and instruction to students in the appropriate use of such resources. Staff will consult the Network Manager and Senior Leadership Team for advice on content, training and appropriate teaching levels consistent with the school's IT programme of study.

Independent student use of telecommunications and electronic information resources is not advised and will only be permitted upon submission of permission and agreement forms by parents of students and by students themselves.

Access to on-line resources will enable students to explore thousands of libraries, databases, and bulletin boards while exchanging messages with people throughout the world. The school believes that the benefits to students from access to information resources and increased opportunities for collaboration exceed the disadvantages. But ultimately, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources. To that end, the school supports and respects each family's right to decide whether or not to apply for independent access.

The school's Network Manager together with the Senior Leadership Team will prepare appropriate procedures for implementing this policy and for reviewing and evaluating its effect on teaching and learning.

Instructions for all computer users in School

Access to the school network, the Internet, email and standalone computers will be provided, but only on the understanding that you 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 any time from anywhere on the school network without you knowing about it.

- Users are responsible for good behaviour on the computers just as they are in a classroom or a school corridor. General school rules apply.
- All users should be aware that their username and password 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 password. If doing shared work you must keep a copy of the work on your own Pen Drive or in your network drive home folder, in case your working partner is absent from school.
- Do not reveal your password to anyone. If you think someone has learned your password then change it immediately, or request for it to be changed.
- Do not trespass in others' folders, work or files. Do not use a computer that is logged on as someone else, use only your own username and password
- 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.
- Please do not spend too long sending/receiving email messages - someone else is usually waiting to use the computer. You should not waste valuable resource time sending trivial emails to another person in the school, or to anyone else for that matter.
- It is your responsibility to save important work files to your 'My Documents' area or your own pen drive.
- If a "virus alert" occurs when transferring work files from the internet, e-mail or a pen drive please inform a member of staff immediately.
- Intentional damage to computers, computer systems or computer networks, including unauthorised damage or interference to any files is not permitted

- Programs must not be installed on a computer except by the Network Manager or a qualified technician. Do not bring in programs on a floppy disk, pen drive or CD Rom 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.

Sanctions

1. Violations of the above rules will result in a temporary or permanent ban on your use of the school network.
2. Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour.
3. When applicable, police or local authorities may be involved.

Internet use

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

Password Security.

The following applies to all THS computer account holders and relates to accounts on the THS Community Connect 4 network (CC4), THS email (@tarletonhigh.lancs.sch.uk), Moodle, e-Portal and Facility. This policy does not apply to Finance users and users of the Lancashire County Council Schools' Portal as those systems already have separate password procedures.

All user account passwords must meet the following complexity requirements:

1. Must not contain the user's account name or parts of the user's full name that exceed two consecutive characters.
2. Must be at least six characters in length.
3. Must contain characters from three of the following four categories:
 - I. English uppercase characters (A through Z)

- II. English lowercase characters (a through z)
- III. Base 10 digits (0 through 9)
- IV. Non-alphabetic characters (for example, !, \$, #, %)

Implementation:

The CC4 computer network will be set to enforce the complexity requirements with a security setting and the password rule is enforced when passwords are changed or created. All other accounts (THS email, Moodle, e-Portal and Facility) will comply with this policy as a matter of rule.

All system users will be reminded it is important to keep passwords secure, they must not divulge them to any other individual, and passwords must be changed termly.

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.
- You should be aware that a member of staff can view your computer screen at any time from anywhere on the school network without your knowledge.
- During lessons, staff will guide students toward appropriate materials. Outside of lessons, families 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 your school 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 school).**
- **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).
- Revealing any personal information, the home address or personal phone numbers of yourself or other people. Completing questionnaires or subscription forms.

- Downloading games or other executable programs. Downloading unlicensed music or video content, including mp3's and music 'ripped' from audio CD's.
- Intentionally wasting limited resources on unnecessary or unauthorised activities.
- Private use of the Internet or email service without advanced permission.
- Use of commercial activities by for-profit institutions.
- Carrying on a private business.
- Undertaking financial transactions unless authorised to do so.

Check with a member of the ICT department before:

- Opening unidentified email attachments.

Sanctions

1. Violations of the above rules may result in a temporary or permanent ban on Internet use.
2. Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour.
3. When applicable, police or local authorities may be involved.

School Network Security

The school network is a valuable resource that is freely available to all students and staff from the majority computers situated throughout the school. Due to the wide variety of uses by well over a thousand users, a number of precautions have to be taken to help ensure that the system is kept available and in full working order:

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 any time from anywhere on the school network without the user knowing about it.
- **Tarleton Academy's computer network is equipped with a program that is able to detect inappropriate behaviour on the computer system. Violations of this Acceptable Use Policy 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**

Network User Access

- Access to the school network is available from any network station during the normal school day. The Network Management team are responsible to ensure 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 this school.
- 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 is continually audited for each user.

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 a Pen Drive or CD Rom left in the disk drive.
- A weekly search is made for any executable programs, zip files, 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 off site for longer periods of time before reuse.
- Students may also be encouraged to perform backups of their own files on their own pen drives.
- Station backups are not required. A faulty station can be quickly rebuilt with all the necessary software via files stored centrally on the server.

- The network servers are located within an office. This office is kept locked when not under direct supervision.

Software Inventory

- An inventory is maintained by the Network Management team containing a record for each item of software that is available for use on the network and the number of licences held.
- Licences must be sent to the Network Managers office for filing in case proof of ownership is required.
- It is important that staff seek the advice of the Network Manager before purchasing software.

Access to Software

- All users receive desktop icons and start-menu-shortcuts to all the main application programs and common utilities.
- Students have read-only access to shared documents but may copy them for their own use.
- Sites visited on the Internet are audited, and filtered - see our Internet Security Policy.

Hardware Security

- An inventory of all equipment together with make, model, serial number, date of purchase and location is maintained by the Network Management team.
- Rooms with computers must be locked overnight and when not in use, where possible.
- All computer rooms and corridors are monitored by the school alarm system after school hours.
- All major items are security marked to identify them as the property of the school.
- Mice, keyboards and other power cables are security tagged to the computer in order to discourage their removal.
- All users should ensure adequate care of equipment. Misuse or damage of equipment may result in persons being liable for replacement or repair costs and the suspension or removal of Network Access rights.

Electrical Safety

- All equipment attached to the main electrical supply is safety tested regularly, in compliance with government regulations.

- The servers operate from an Uninterruptible Power Supply (UPS) to protect against power surges and blackouts.

Fire Protection Measures

- Waste material should be frequently removed from the computer areas.
- A carbon dioxide (CO₂) fire extinguisher is required in all main computer rooms and staff should ensure that they know where it is and how to use it.

Internet Security

The Internet is a valuable resource that is freely available to all students and staff on all our school network stations. Due to the "unsuitable" nature of some material on the Internet and the possible misuse of the Internet or email, a number of precautions have to be taken to help ensure that the system is used responsibly:

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

- Access to many, if not most sites considered to contain "unsuitable" material is prevented by a filtering system used by our Internet Service Provider. 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.
- Chat Rooms are not considered to be a suitable use of a busy school network system nor of anyone's time in school. Our Internet Service Provider also now filters them. An exception to this rule is that access to the 'Moodle' (the school's Virtual Learning Environment) or other approved interfaces are allowed, however, misuse of Moodle will result in suspension or removal of Moodle access rights and possible further disciplinary action.
- Precautions are taken to reduce the chances of infection by computer viruses via the Internet or email. The anti-virus software, which is installed on all school network stations, is updated every day.
- Users found actively searching for "unsuitable" material or sending offensive email messages will have their access to the Internet denied and further action 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

Mobile Phone Use

The possession of mobile phones by students is acceptable to the school. We recognise that a mobile phone is a means of effective communication by students who may choose to stay at school for an extra-curricular activity or visit their friends. Nevertheless, there are a number of simple rules about use of mobile phones on school premises.

- Mobile phones should be switched off in all lessons, assemblies and when students are walking between lessons.
- The use of mobile phones to intimidate other students is clearly unacceptable and constitutes a form of bullying.
- The school carries no insurance to cover the loss of any private possessions and therefore we cannot reimburse any student for the loss of a mobile phone whilst in school.
- The use of camera phones can lead to legal difficulties when students are photographed without permission, therefore the school's strong advice is that camera phones should not be used to take photographs on the school's premises.
- The use of mobile phones to transmit obscene/unacceptable images and video footage is strictly forbidden.

The Governing Body will review this policy on an annual basis.

Adopted by the Governing Body

Date: 29th November 2011

Appendix 1

Parents' permission letter

Dear Parent,

As part of the school's technology programme we offer students supervised access to computers including the internal network and the Internet, the global network of computers. Before being allowed to use the computers, all students must obtain parental permission and both they and you must sign and return the enclosed form as evidence of your approval and their acceptance of the school rules and associated policies.

Access to computers will enable students to explore thousands of libraries, databases, and bulletin boards. Families should be warned that some material accessible via the Internet may contain items that are illegal, defamatory, inaccurate or potentially offensive to some people.

Whilst our aim for Internet use is to further educational goals and objectives, students may find ways to access other materials as well. We believe that the benefits to students from access to the Internet, in the form of information resources and opportunities for collaboration, exceed any disadvantages. But ultimately, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources. To that end, the school supports and respects each family's right to decide whether or not to apply for access.

Whilst on school premises, staff will guide students toward appropriate materials. Outside of school, families bear the same responsibility for such guidance as they exercise with information sources such as television, telephones, movies, radio and other potentially offensive media.

We would ask that you read the enclosed policy documents and then complete the permission form which follows.

Yours sincerely

Lesley Gwinnett

Headteacher

Appendix 2

Network Use Permission Form

Please complete and return this form to the Network Manager

As a school computer user, I agree to comply with the school rules on their use. I will use the computers in a responsible way and observe all the restrictions and policies explained to me in the accompanying documentation.

Name of Computer User (e.g John Smith) _____

Username (e.g. 10SmithJ) _____ (Provided by the Network Manager)

Signature _____ Date: ___/___/___

If applicable: Tutor Group _____

Parent or Guardian (**applicable to users under the age of 16**)

I have read and understood the Tarleton Academy Acceptable Use Policy. As the parent or legal guardian of the student signing above, I grant permission for my son or daughter to use school computers, electronic telecommunications, mail and the Internet. I understand that students will be held accountable for their own actions. I also understand that some materials on the Internet may be objectionable and I accept responsibility for setting standards for my daughter or son to follow when selecting, sharing and exploring information and media.

Parent Signature _____ Date ___/___/___

What is the Internet?

The Internet is a large number of computers all over the world linked together with cables. In most cases, each of these computers is also linked locally to a number of other computers, in a **local network**. It is possible for someone using one of these computers to access information on any of the other computers. This system was established by those working in Universities and Government organisations for the fast and efficient transfer of largely text-based information around the world directly from one computer to another.

It is possible for other people, outside these local networks, to connect to the Internet by using standard telephone lines between their computers and those already connected to the Internet. A number of companies specialise in providing this service for a fee.

What is the World Wide Web?

To make the appearance of information available through the Internet more attractive, and to assist people in finding information more easily, it is now possible for special pages of information to contain text, colours, and pictures, sound and even video. These pages, collectively, make up what is known as the World Wide Web. Most of these pages include information on the location of other pages on the World Wide Web, and it is possible to follow up links between pages with similar or related content. Moving from one page to another, regardless of where in the world they might be located, is called browsing, or surfing the net or web. Many of these Web pages contain information that may be useful in the classroom, and it is presented in a way which is often easy to use.

A number of UK suppliers including AOL, BT, Research Machines and the TCTrust, offer schools the facility of keeping their own pages on the Internet. These school "home pages" might describe the school's activities to outsiders or explain project work that students are involved in. Our URL is: <http://www.tarletonhighschool.co.uk>

What is Electronic Mail (E-mail)?

This is merely a way of sending messages from one person to another via the Internet. Each Internet user can have a unique e-mail address (such as anybody@msn.com) and by sending a message to this address, the recipient can read the message the next time he or she connects to the Internet. Internet e-mail addresses are usually provided along with a school's connection to the Internet and normally individual students will not have their own email address.

What are News Groups?

These are collections of messages written for public readership rather than addressed to an individual. Each collection, or group, of messages is about a particular subject or theme. Individuals can reply to these messages, and these replies are also public. In this way it is possible to track a multi-way conversation about an important issue of the day. At present there are more than 10,000 different topics available for discussion, from specialist science research to support groups for asthma to fans of James Bond movies. Most of the press

concern for pornography on the Internet refers to newsgroups but they are the easiest for school Internet providers to police.

What are the dangers of the Internet referred to in the media?

It is true that there is some material on the Internet that would be offensive to most people, such as pornography, racist and fascist material and children can access this if using the Internet unsupervised. The main educational providers try to 'filter' known offensive locations of material of this kind, but there is too much for this filtering to be totally effective, and the locations change frequently. The only way to block access to this kind of material is to have a restricted range of pages available, in which case many of the advantages of the global and dynamic nature of the Internet may be lost. It is a feature of the Internet that the information available is free. Increasing restrictions will undoubtedly lead to systems of charging for access to specific material, in addition to the other costs described. An alternative system is to educate students and encourage an acceptable use policy and partnership between home and school in dealing with the less savoury side of Internet use.

How can I get more information?

There are many magazines in newsagents that cater for beginners-advanced use of the Internet. If you have any specific questions please contact the school and ask for the Network Manager.