The Leigh Academy
Acceptable Use Policy
Network Usage

Networked resources, including Internet access, are potentially available to students and staff in the academy. All users are required to follow the conditions laid down in this policy. Any breach of these conditions may lead to withdrawal of the user's access, monitoring and or retrospective investigation of the users use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

These networked resources are intended for educational purposes, and may only be used for legal activities consistent with the rules of the academy. Any expression of a personal view about the academy or County Council matters in any electronic form of communication must be endorsed to that effect. Any use of the network that would bring the name of the academy or County Council into disrepute is not allowed.

The academy expects that staff will use new technologies as appropriate within the curriculum and that staff will provide guidance and instruction to students in the use of such resources. Independent student use of the Internet or the Academy's VLE must only be for related Academy Curriculum tasks, or as directed by a member of staff. All computer systems will be regularly monitored to ensure that they are being used in a responsible fashion.

CONDITIONS OF USE

Personal Responsibility

Access to the networked resources is a privilege, not a right. Users are responsible for their behaviour and communications. Staff and students will be expected to use the resources for the purposes for which they are made available. Users are to take due care with the physical security of hardware they are using. Users will accept personal responsibility for reporting any misuse of the network to their appropriate College SLT.

Acceptable Use

Users are expected to utilise the network systems in a responsible manner. It is not possible to set hard and fast rules about what is and what is not acceptable but the following list provides some guidelines on the matter:

NETWORK ETIQUETTE AND PRIVACY

Users are expected to abide by the rules of network etiquette. These rules include, but are not limited to, the following:

1. Be polite – never send or encourage others to send abusive messages.
2. Use appropriate language – users should remember that they are representatives of the academy on a global public system. Illegal activities of any kind are strictly forbidden.
3. Do not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.
4. Privacy – do not reveal any personal information (e.g. home address, telephone number) about yourself or other users. Do not trespass into other users files or folders.
5. Password – do not reveal your password to anyone. If you think someone has learned your password then contact the IS Network manager who will change the password immediately.
6. Electronic mail – Is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities. Do not send anonymous messages.
7. Disruptions – do not use the network in any way that would disrupt use of the network by others.
8. Students will not be allowed access to unsupervised and/or unauthorised chat rooms and should not attempt to gain access to them.
9. Staff or students finding unsuitable websites through the academy network should report the web address to the IS Manager who will arrange to have them blocked.
10. Do not attempt to visit websites that might be considered inappropriate. Such sites would include those relating to illegal activity, All sites visited leave evidence. Downloading some material is illegal and the police or other authorities may be called to investigate such use.
11. Unapproved system utilities and executable files will not be allowed in students' work areas or attached to e-mail.
12. Files held on the academy's network may be checked by the members of the IS department.
13. .It is the responsibility of the User (where appropriate) to take all reasonable steps to ensure compliance with the conditions set out in this Policy document, and to ensure that unacceptable use of the Internet/Network does not occur.

UNACCEPTABLE USE

Examples of unacceptable use include but are not limited to the following:

- Users must login with their own user ID and password, where applicable, and must not share this information with other users. They must also log off after their session has finished.

- Users finding machines logged on under other users username should log off the machine whether they intend to use it or not.
- Accessing or creating, transmitting, displaying or publishing any material (e.g. images, sounds or data) that is likely to cause offence, inconvenience or needless anxiety.
- Accessing or creating, transmitting or publishing any defamatory material.
- Receiving, sending or publishing material that violates copyright law. This includes through Video Conferencing and Web Broadcasting.
- Receiving, sending or publishing material that violates Data Protection Act or breaching the security this act requires for personal data.
- Transmitting unsolicited material to other users (including those on other networks).
- Unauthorised access to data and resources on the academy network system or other systems.
- User action that would cause corruption or destruction of other users' data, or violate the privacy of other users, or intentionally waste time or resources on the network or elsewhere.

Additional guidelines

- Users must comply with the acceptable use policy of any other networks that they access.
- Users should only communicate electronically with students via the student and staff Academy created email accounts and via the Academy Google classrooms and communities
- Users must not download software without approval from the network manager

SERVICES

There will be no warranties of any kind, whether expressed or implied, for the network service offered by the academy. The academy will not be responsible for any damages suffered while on the system. These damages include loss of data as a result of delays, non-deliveries, or service interruptions caused by the system or your errors or omissions. Use of any information obtained via the network is at your own risk.

NETWORK SECURITY

Users are expected to inform the network manager/College Principal immediately if a security problem is identified. Do not demonstrate this problem to other users. Users must login with their own user id and password, where applicable, and must not share this information with other users. Users identified as a security risk will be denied access to the network.

PHYSICAL SECURITY

Staff users are expected to ensure that portable ICT equipment such as laptops, iPads, digital still and video cameras are securely locked away when they are not

being used. Items that need to be left over breaks and lunchtimes for example will need to be physically protected by locks and or alarms.

WILFUL DAMAGE

Any malicious attempt to harm or destroy any equipment or data of another user or network connected to the academy system will result in loss of access, disciplinary action and, if appropriate, legal referral. This includes the creation or uploading of computer viruses. The use of software from unauthorised sources is prohibited.

MEDIA PUBLICATIONS

Written permission from parents or carers will be obtained before photographs of students are published. Named images of students will only be published with the separate written consent of their parents or carers.

Publishing includes, but is not limited to:

- the academy website
- the Local Authority web site,
- web broadcasting,
- TV presentations,
- Newspapers.

Students' work will only be published (e.g. photographs, videos, TV presentations, web pages etc) if parental consent has been given.

Updated by JCO 22/08/16 - next review July 2017

The Leigh Academy
Mobile Phone and Handheld Device Acceptable Use Policy

Mobile Phones and Handheld Devices

Rationale

This policy sets out what is 'acceptable' and 'unacceptable' use of handheld devices including mobile phones by the whole academy community (students, staff and visitors) while they are at the Academy or undertaking academy activities away from school.

This applies to all individuals who have access to personal and/or work-related handheld devices within the broadest context of the setting. It includes children and young people, parents and carers, practitioners, managers, volunteers, students, governors, visitors, contractors and community users. This list is not exhaustive.

It is to be recognised that it is the enhanced functions of many handheld devices that will give the most cause for concern; and which should be considered the most susceptible to potential misuse. Examples of misuse include the taking and distribution of indecent images, exploitation and bullying.

It must be understood that should handheld devices be misused, there will be a negative impact on an individual's safety, dignity, privacy and right to confidentiality. Such concerns are not to be considered exclusive to children and young people, so the needs and vulnerabilities of all must be respected and protected.

Mobile phones and handheld devices can also cause an unnecessary distraction during the academy day and are often to be considered intrusive when used in the company of others.

The purpose of this policy is to prevent unacceptable use of mobile phones, camera-phones and other hand held devices by the academy community, and thereby to protect the Academy's staff and students from undesirable materials, filming, intimidation or harassment.

1. Protocols

1.1 Mobile phones and personally-owned mobile devices brought in to school are The responsibility of the device owner. The Academy accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.

1.2 Student mobile phones, which are brought into the academy, must be turned off (not placed on silent) and stored out of sight on arrival at school. They must remain turned off and out of sight in lessons unless students are required to use them to support their learning at the direction of the teacher. Staff members may use their phones during school break times. All visitors are requested to keep their phones on silent.

1.3 The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where the Principal has explicitly agreed it otherwise. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Principal is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.

1.4 The Academy reserves the right to search the content of any mobile or handheld devices on the academy premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying.

1.5 Where parents/carers or students need to contact each other during the school day, they should do so only by telephone through the relevant College Admin.

1.6 Mobile phones and personally-owned devices are not permitted to be used in certain areas within the Academy, e.g. changing rooms and toilets.

1.7 Mobile phones and personal handheld devices will only be used during lessons or formal academy time as part of an approved and directed curriculum-based activity with consent from a member of staff.

1.8 Mobile phones and personal handheld devices should not be used to play personal music during lessons or formal academy time and should therefore not be connected to any Academy device for purposes of charging batteries.

1.9 No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.

2. Students' use of personal mobile phones and handheld devices

2.1 Students will be reminded regularly of the acceptable use of mobile phones and handheld devices during the academy day. Inappropriate use of mobile and handheld will be dealt with as per The Academy Rewards and Consequences Policy.

2.2 If a student breaches the academy policy then the phone or device will be confiscated and will be held in a secure place in the main Academy office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.

2.3 Phones and devices must not be taken into examinations. Students found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.

2.4 If a student needs to contact his or her parents or carers, they will be allowed to use a phone in their College Admin office. Parents are advised not to contact their child via their mobile phone during the academy day, but to contact the academy office.

2.5 Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.

2.6 Students, under the instruction of their teacher may use their mobile phones and handheld devices to store or record their work. The Academy is not responsible for any work stored on mobile phones and handheld devices.

2.7 Students may use their mobile phones and handheld devices for personal use during break and lunchtimes provided that students follow the protocols outlined in section 1.

3. Staff guidelines for the use of personal devices

These guidelines are designed to support staff and to remind staff of the responsibility they have with regards to the Safeguarding of students. All staff new to The Academy undergo detailed Leigh Academies Trust Safeguarding training and the use of mobile devices is covered as part of this Professional Development.

3.1 Staff should avoid using their own mobile phones or devices for contacting students, young people or their families within or outside of the setting in a professional capacity.

3.2 Mobile phones and personally-owned devices should be switched off or switched to 'silent' mode.

3.3 If members of staff have an educational reason to allow students to use mobile phones or a personally-owned device as part of an educational activity the use of the device should be monitored carefully by the member of staff authorising the student to do so.

3.4 Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and should only use work-provided equipment for this purpose.

3.5 If a member of staff breaches the school policy then disciplinary action may be taken.

Updated by SWT 24/04/16 next review 24/04/17