DAUBENEY ACADEMY

E Safety – ICT Acceptable Use Policy (AUP)

STAFF

Approved by FGB – 12.02.15

The use of ICT in schools for both teaching, management and administration purposes has increased tremendously in recent years. Networked resources, including Internet access and access to the schools Virtual Learning Environment (VLE), are available to staff and pupils in the school. 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 and or retrospective investigation of the user's use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

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

The school expects that staff will use all technologies as appropriate within the curriculum and that staff will provide guidance and instruction to pupils in the use of such resources. All computer systems will be regularly monitored to ensure that they are being used in a responsible fashion.

Personal Responsibility

Access to the networked resources is a privilege, not a right. Users are responsible for their behaviour and communications. Staff 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 the Senior Information Risk Officer (SIRO) and/or Information Asset Owner (IAO).

Security & Safety

- Rules for Internet access will be posted in all rooms where computers are used;
- Staff are informed that Internet and email use will be monitored and if needs be traced to the individual user;
- The School may place staff that are under reasonable suspicion of misuse under retrospective investigation. Alternatively the school will actively monitor users suspected of misuse. This misuse may be in terms of time or content;
- A module on responsible Internet use will be included in the Citizenship/KS2 and KS3 Computing programme of study covering both school and home use;
- Schools should inform the IT Technician 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 and must not share this information with anyone. Users are responsible for their password security and must take all reasonable safeguards to protect it. Users will be held accountable for any misuse recorded under their account details if reasonable care was not demonstrated;
- Users identified as a security risk will be denied access to the network;
- Methods to identify, assess and minimise risks will be reviewed regularly;

The school will keep an up to date record of all staff that are granted Internet access. For instance, a member of staff may leave. Those managing school networks need up to date lists of current staff that are to be given access. In addition to this they will need to be informed of staff leaving so their accounts can be at first disabled and ultimately deleted.

The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

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 (Internet and Email)

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

- Professional conduct must be maintained at all times;
- Be polite – never send or encourage others to send abusive messages. Defamatory comments could result in legal action. E-mail has been used successfully as evidence in libel cases;
- Use appropriate language – users should remember that they are representatives of the school on a global public system. Illegal activities of any kind are strictly forbidden;
- Do not use language that could be calculated to incite hatred against any ethnic, religious or other minority group;
- Do not view, send or retain any offensive or illegal material. This includes any jokes or content such as that which contains racist terminology, violence, pornography or any material that might constitute harassment;
- 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;
- Password – do not reveal your password to anyone. If you think someone has learned your password then contact the IT Technician. Users are responsible for any misuse recorded under their username;
- Electronic mail is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities;
- Disruptions – do not use the network in any way that would disrupt use of the network by others;
- Staff finding unsuitable websites through the school network should report the web address to the IT Technician as soon as reasonably possible;
- Do not introduce portable media devices such as pen drives, into the network without having them checked for viruses;
- Do not attempt to visit websites that might be deemed inappropriate by the school. All sites visited leave evidence on the network if not on the computer. Downloading some material is illegal and the police or other authorities may be called to investigate such use;

- Unapproved system utilities and executable files will not be allowed in staff work areas or attached to e-mail;
- Files held on the school's network will be regularly checked by the IT Technician;
- It is the responsibility of the User 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/Intranet does not occur;
- The virtual learning environment (It's Learning) must be used to support learning. Any misuse could result in this provision being removed from any user. In particular, resources taken from the web must give copyright permission for VLE use.

Chat Rooms

Chat is a conferencing application offering instantaneous exchange of text and images between groups of users via the Internet.

Chat sites are banned under the school filtering system. Under exceptional circumstances, a chat site could be made available provided the school takes the following measures: -

- The teacher would moderate such chat facilities and the teacher would only at times permit access;
- Unauthorised persons would not know of the chat conference existence and therefore would not be able to gain access;
- The importance of chat room safety will be emphasised to pupils;
- The chat site is only made available to staff for a specific professional purpose.

Forums

A forum is an on-line discussion group where people exchange ideas about a common interest or theme. Forums that are made available to pupils using the internet need to be moderated to ensure correct use and no offensive posts are made. This means that the responsible teacher will have to approve every post that is made to the forum. A forum available over the Internet will require a level of access control, whereby only authorised/registered users can use the forum. Moderators must ensure that they are qualified in the subject to which they are responding and take reasonable precautions not to give out wrongful advice.

The following rules, inline with other AUP areas, need to be communicated:

- Personal attacks, foul language, violation of privacy or abusive behaviour will not be tolerated and will be reported;
- Spamming and advertisements of any type, as well as the use of programs such as scripts, worms or Trojan horses will not be tolerated. Any type of participation in this type of activity will mean you will be reported and the possible termination of your account.

Please note, forums' owners are able to contact the local authority to report misuse of forum facilities, and we can trace back the users to the school.

Additional E-mail protocols

- All users must follow the guidelines set out in the Network etiquette section of this document;
- Staff may only use approved e-mail accounts on the school system. Access in school to external personal e-mail accounts may be blocked.
- The forwarding of chain letters is not permitted;
- An email sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
- Messages that are likely to bring the school into disrepute should not be sent;
- Do not open suspect emails or attachments; they may contain a virus;
- Communication with pupils should take place within professional boundaries and staff should avoid any personal subject matter. Staff should be circumspect in their communications with pupils so as to avoid any possible misinterpretation of their motives.

UNACCEPTABLE USE

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

- Users must login with their own user ID and password 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;
- Sharing of digital recordings by any device (video, photos or sound).
- Searching for, looking at, creating or publishing offensive material;
- Accessing or creating, transmitting or publishing any defamatory material;
- Receiving, sending or publishing material that violates copyright law;
- 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 school 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;
- Users must not download software without approval from the IT Technician;
- Spending excessive amounts of time using the internet or email for non-school / work related reasons. Incidental personal use is permitted provided it complies with these protocols and does not interfere with work or study.

Failure to adhere to these protocols may result in loss of access to the Internet as well as other disciplinary action.

SERVICES

There will be no warranties of any kind, whether expressed or implied, for the network service offered by the school. The school 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.

WILFUL DAMAGE

Any malicious attempt to harm or destroy any equipment or data of another user or network connected to the school 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 pupils are published. Named images of pupils will only be published with the separate written consent of their parents or carers.

Security and Virus Protection

Any malicious attempt to harm or destroy any equipment or data owned by another user 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.

Network Security

Users are expected to employ good password practice when using the network. This includes keeping personal passwords secure and always logging off after use.

Users are also expected to inform the IT Technician 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.

The IT Technician will ensure that:

- The server operating system must be secured to a high level;
- Anti Virus software is both installed throughout the network and kept up to date. This includes taking steps to allow staff laptops to receive updates either at home or in school;
- Steps are taken to ensure that Windows critical updates are both downloaded and installed on a regular basis;
- Wireless networks use at least WEP (Wired Equivalent Privacy) encryption to prevent unauthorised access to their network. They may also wish to only allow access to specific MAC addresses (Short for Media Access Control address, a hardware address that uniquely identifies each computer on the

network) and/or putting timers on the access points so they only work during school operating hours.

Hardware Security

- All costly ICT equipment is security marked in a concealed area on the device and serial numbers are inventoried;
- The IT Technician must ensure that network servers are located securely and physical access restricted;
- Staff users are expected to ensure that portable ICT equipment such as laptops, 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. Users identified as a security risk may be denied access to these types of equipment.
- All portable ICT equipment removed from the school by a staff member must be logged and approved on the school's 'Record of Equipment Loaned or Removed From School'.

Passwords / Usernames

- Users must be vigilant at all times regarding their password security. It is advised that staff users regularly change their passwords every term. Staff will be prompted once every term to change their passwords. Passwords should contain a mixture of lower and uppercase letters, characters, numbers and symbols. E.g. PassWorD123$%^;
- Users must always log off when finished;
- Users must always lock the computer if they are away from the computer [Windows key + L = 'lock computer']. To get back onto their computer [Ctrl Alt + delete]. Users finding machines logged on under other users' username should log off the machine whether they intend to use it or not. A locked computer can only be unlocked by the person logged onto it;
- It is the users' explicit responsibility to ensure password security. Any computer misuse found under a username will be the responsibility of the named user, unless all reasonable care can be demonstrated.

The terms username and password in this ICT policy concern any software or hardware application linked to Daubeney Academy, e.g.

- Computer access to the school network;
- SIMS;
- VLE / Its Learning;
- Outlook ;
- Governmental websites.

E-safety monitoring

- **Identify risks** – We aim to identify network and website use by all users. All applications are covered, including chat rooms and email. It also covers all documents (e.g. Word, PowerPoint), whether they are viewed, printed or

typed. Even unsaved or deleted material is captured if it contains an unacceptable word or phrase;

- Capture evidence - **A record is taken of any incident that might indicate a problem or concern.** This might be as simple as swearing or a more serious issue such as bullying, racist language or grooming online. It might also show when a banned or unsuitable website has been accessed. A screenshot shows what was on screen at the time, along with the identity of the user, time and date. Such evidence can be used to follow up with the user later.
  - **Follow up** - If the situation is potentially serious, staff are automatically alerted. The violations can be reviewed at any time from any PC. This helps the right action to be taken, whether supporting a victim of bullying, protecting a vulnerable child or confronting a pupil who has used a computer inappropriately;

  - **Managing behaviour** - Pupils must agree to a code of conduct. This lays out clear guidelines on what is appropriate behaviour. It also provides a reminder that any misuse will be identified and acts as a powerful deterrent against ICT misuse. Pupils learn how to act responsibly, what behaviour is acceptable or safe and what is not. It also reduces the temptation to surf the internet or email friends in lessons.

NB: For an overview of acceptable use and school procedures in the event of **misuse please see below.**

	Staff & other adults			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed
Mobile phones may be brought to school	✓			
Use of mobile phones in lessons				✓
Use of mobile phones in social time		✓		
Taking photos on mobile phones or personal camera devices				✓
Use of hand held devices eg PDAs, PSPs (school owned equipment)	✓			
Use of personal email addresses in school, or on school network		✓		
Use of school email for personal emails		✓		
Use of chat rooms / facilities		✓		
Use of instant messaging (MSN)		✓		
Use of social networking sites		✓		
Use of blogs (It's Learning only)	✓			

Mobile phones should be set to silent/vibrate when in earshot of public places within the school

Approved by FGB – 12.02.15

Staff User Actions

		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**child sexual abuse images**					✓
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					✓
	adult material that potentially breaches the Obscene Publications Act in the UK					✓
	criminally racist material in UK					✓
	pornography				✓	
	promotion of any kind of discrimination				✓	
	promotion of racial or religious hatred				✓	
	threatening behaviour, including promotion of physical violence or mental harm				✓	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				✓	
Using school systems to run a private business					✓	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Talkstraight and / or the school					✓	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					✓	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					✓	
Creating or propagating computer viruses or other harmful files					✓	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet					✓	
On-line gaming (educational)		✓				
On-line gaming (non educational)			✓			
On-line gambling					✓	
On-line shopping / commerce (at your own risk)			✓			
File sharing					✓	
Use of social networking sites			✓			
Use of video broadcasting eg YouTube			✓			

Approved by FGB – 12.02.15

Approved by FGB – 12.02.15

Staff Actions / Sanctions

Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action	Incident Logged
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		✓	✓		✓	✓		✓	✓
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email		✓			✓	✓			
Unauthorised downloading or uploading of files		✓			✓	✓			
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	✓	✓			✓	✓			
Careless use of personal data eg holding or transferring data in an insecure manner	✓				✓	✓			
Deliberate actions to breach data protection or network security rules		✓			✓	✓			✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		✓			✓	✓		✓	✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		✓			✓	✓		✓	✓
Using personal email(such as Hotmail) / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		✓			✓	✓		✓	✓
Actions which could compromise the staff member's professional standing		✓				✓			
Actions which could bring the school community into disrepute or breach the integrity of the ethos of the school		✓				✓			✓
Using proxy sites or other means to subvert the school's filtering system		✓			✓	✓			✓
Accidentally accessing offensive or pornographic material and failing to report the incident		✓	✓		✓	✓		✓	✓
Deliberately accessing or trying to access offensive or pornographic material		✓	✓		✓	✓	✓	✓	✓
Breaching copyright or licensing regulations		✓				✓			

Approved by FGB – 12.02.15

Continued infringements of the above, following previous warnings or sanctions		✓				✓		✓	✓

Approved by FGB – 12.02.15