DAUBENEY ACADEMY

E Safety – ICT Acceptable Use Policy (AUP)

PUPILS

Approved byFGB – 12.02.15

	Pupils			
	Allowed	Allowed at certain times	Allowed with staff permission and supervision	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 byFGB – 12.02.15

Pupil 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					✓
	Explicit sexual content				✓	
	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					✓	
File sharing					✓	
Use of social networking sites					✓	

Approved byFGB – 12.02.15

Use of video broadcasting eg YouTube				✓	

Approved byFGB – 12.02.15

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Headteachers	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion	Incident Logged
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	✓	✓	✓		✓	✓	✓	✓	✓	✓
Unauthorised use of non-educational sites during lessons	✓				✓		✓	✓		✓
Unauthorised use of mobile phone / digital camera / other handheld device	✓	✓				✓		✓	✓	
Unauthorised use of social networking / instant messaging / personal email	✓	✓			✓	✓		✓	✓	✓
Unauthorised downloading or uploading of files	✓				✓			✓		✓
Allowing others to access school network by sharing username and passwords	✓				✓	✓		✓		✓
Attempting to access or accessing the school network, using another student's / pupil's account		✓			✓	✓		✓		✓
Attempting to access or accessing the school network, using the account of a member of staff	✓	✓	✓		✓	✓	✓	✓	✓	✓
Corrupting or destroying the data of other users	✓	✓	✓		✓	✓	✓	✓	✓	✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓	✓		✓	✓	✓	✓	✓	✓
Continued infringements of the above, following previous warnings or sanctions	✓	✓	✓		✓	✓	✓	✓	✓	✓
Actions which could bring the school into disrepute or breach the integrity of the community ethos of the school	✓	✓	✓		✓	✓	✓	✓	✓	✓
Using proxy sites or other means to subvert the school's filtering system	✓	✓	✓		✓	✓	✓	✓	✓	✓
Accidentally accessing offensive or explicit sexual content material and failing to report the incident	✓	✓			✓	✓	✓	✓		✓
Deliberately accessing or trying to access offensive or explicit sexual content material	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Approved byFGB – 12.02.15

Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		✓			✓	✓	✓	✓		✓

Your Responsibility

Access to the networked resources\computers is a privilege, not a right. Pupils are responsible for their behaviour and communications. Pupil users are to take care of the equipment they are using.

Security & Safety

- Rules for Internet use are available on the learning platform;
- Internet and email use will be monitored and can be traced to the individual user;
- The School may place pupils that are under reasonable suspicion of misuse. 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 lessons covering both school and home use;
- Pupil users should inform the IT Technician immediately if a security problem is identified. Do not demonstrate this problem to other users;
- Pupil 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;
- Pupil 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 pupils who are granted Internet access.

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

Acceptable Use

Pupil users are expected to utilise the network system 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:

These rules include, but are not limited to, the following:

- 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, explicit sexual content 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;
- 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;
- Pupils 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 considered inappropriate. 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 pupils' 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.

Additional E-mail rules

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately inform a teacher/IT Technician if they receive offensive e-mail;
- Pupils must not reveal details of themselves or others in email communication, or arrange to meet anyone;
- The forwarding of chain letters is not permitted;
- An email sent to an external organisation should be written carefully and authorised before sending;
- 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;

Pupils should also be aware that e-mail is not a secure medium and should not normally be used for sensitive or confidential information.

Chat Rooms

Chat allows users to have instantaneous exchange of text and images via the Internet. Pupils will not be allowed access to unsupervised and/or unauthorised chat rooms and should not attempt to gain access to them. Remember you cannot see the other person you are talking to.

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 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.

The following rules, in line with other AUP areas, will 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.

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's 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). If a pupil is found to have done this, the school may consider recommending a permanent exclusion. This may also be considered if any technology is used for intimidating behaviour or an attempt to bring the school into disrepute;
- The use of social networking sites such as Facebook and Instagram is prohibited;
- 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;
- Spending excessive amounts of time using the internet or email for non-school related reasons.

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

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 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.

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.

The current SIRO is: Mr S Miles

Approved byFGB – 12.02.15

The current IAO is: Mr J Chopping

Approved byFGB – 12.02.15