alechunteracademy
a Saffron Academy Trust school

POLICY DOCUMENT FRONTPAGE

POLICY NAME: E – Safety Policy

DATE ADOPTED: January 2018

DATE GOVERNORS AGREED POLICY: January 2018

REVIEW PERIOD: 1 year

REVIEW RECORD: Next review date January 2019

E-SAFETY POLICY

This E-Safety Policy has been written by the school, based on various guidance documents and to ensure students, staff and guest users are aware of the protocols for using the internet. It should be read in conjunction with the Code of Conduct for Staff, The Behaviour for Learning Policy and the ICT Acceptable Use Policies.

Educational Purpose

The purpose of internet use in school is:

- to raise educational standards,
- to promote student achievement,
- to support the professional work of staff,
- to enhance the school's management information and business administration systems.

Internet use is a part of the statutory curriculum and a necessary tool for staff and students.

The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality internet access as part of their learning experience where they demonstrate a responsible and mature approach to its use, abiding by the E-Safety Policy.

Alec Hunter Academy expects all users to use the internet responsibly and strictly according to the conditions outlined in this policy.

Safeguards

School internet access will be designed expressly for student use and will include appropriate content filtering.

Filtering will be under constant review, with the facility to unblock sites of educational value for staff or students and block access to sites discovered which are outside of the school's Code of Conduct.

Students will be taught what internet use is acceptable and what is not. All students and staff will be bound by this Policy.

Internet access will be planned to enrich and extend learning activities. Staff will guide students in on-line activities that will support the learning outcomes planned for the students' age and maturity.

Unacceptable Use

All Users shall not use the School Internet system to:

- Access web-based chat sites that allow users to make contact with individuals in the outside world without providing sufficient safeguards and protection to young people.
- Access web-based email services other than the service provided by the school.
- Access sites offering internet based SMS services.
- Visit internet sites that might be defamatory or incur liability on the part of the school.
- Upload, download or otherwise transmit (make or distribute) commercial software or any copyrighted materials belonging to third parties outside of the school.
- Reveal or publicise confidential or proprietary information, databases and information contained therein, computer/network access codes and business relationships.
- Intentionally interfere with the normal operation of the Internet connection, including propagation of computer viruses and sustained high volume traffic (sending or receiving of large files, sending or receiving large numbers of small files or any activity that causes undue network congestion), that substantially hinders others' use of the Internet.
- Solicit, represent personal opinions or reveal confidential information or use it in any other way that could reasonably be considered inappropriate.
- Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
    - Pornography (including images, videos, explicit animation or textural descriptions);
    - Promoting discrimination of any kind (including material that promoted intolerance on the basis of gender, sexual orientation or race);
    - Promoting racial or religious hatred;
    - Promoting illegal acts;
    - Promoting drugs or substance abuse (including websites that promote the use, manufacture or distribution of illegal drugs, or sites that promote the abuse of legal drugs or the sale or use of alcohol by minors);
    - Graphic portrayal of violence, including sites that promote violence or self-endangerment, or that contain instruction on the construction, use or sale of weapons of violence.

Social Networking

Parents need to be aware that the internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Students should be encouraged to think about the ease of uploading personal information and the impossibility of removing an inappropriate photo, video, comment or address once posted.

Examples include:

- Blogs;
- Wikis;
- Forums/Bulletin boards;
- Multi-player on line gaming;
- Social networks (e.g. Facebook, Twitter, Instagram, Tumblr, Snapchat)

- Direct/Instant messaging apps (e.g. Snapchat, Whatsapp, Messenger);
- Many others, and others that may evolve that do not exist at present.

The school will take the following steps in relation to the internet at school and outside of school:

- Block/filter access to social networking sites at school;
- Newsgroups will be blocked unless a specified use is approved;
- Students will be advised never to give out personal details of any kind which may identify them or other students or their location. (Examples include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests, clubs, streaming and/or uploading photos/videos of students in school or in uniform;
- The use of information and communication technologies such as e-mail, mobile phone and text messages, instant messaging, defamatory personal web sites and defamatory personal polling websites, to support deliberate, repeated or hostile behaviour by an individual or a group, that is intended to harm others is forbidden and will be dealt with severely.

Parental Guidance

Due to the proliferation of social media sites, we offer the following guidance to parents on their child's use of social media:

- Many social media platforms, especially Facebook, have minimum age restrictions. Facebook has a minimum age of 13. It is strongly recommended that parents adhere to these requirements, as they are in place for the protection of the child;
- Social media platforms also have increased and built-in child-protection features for children aged 13 to 16. If your child has lied about their age to secure a page on these sites, these features may not be activated;
- These features include automatic priority of bullying and harassment notifications; automatic monitoring of uninitiated contact by an adult with no friends in common with any concerns forwarded to law enforcement;
- The average child on Facebook has 300+ friends. It is important to discuss with your child the implications of a "friend" on Facebook, and security features they need to place on their account.

Useful links

- Essex Safeguarding Children Board: http://www.escb.co.uk/en-gb/parentscarers/stayingsafeonline.aspx
- NSPCC Share Aware: https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety
- Net Aware: https://www.net-aware.org.uk/#
- UNICEF – Growing Up Online: http://www.unicef.org/endviolence/endviolenceonline/files/UNICEF Growing-up-online.pdf
- Parent Info (Lots of useful links on the "Experts" tab): http://parentinfo.org/
- Marie Collins Foundation (for information on chat room safety, grooming, cyber bullying, internet stalking and internet safety): http://www.mariecollinsfoundation.org.uk/useful-links.

- Think U Know (for information on which sites are safe or not safe online): www.thinkuknow.co.uk
- BBC Bitesize activity (KS3 students): http://bbc.co.uk/bitsize/ks3/ict/history impact ict/safety/activity/
- Child Exploitation and Online Protection Centre (CEOP): https:www.ceop.police.uk/safety-centre/Parents/
- UK Safer Internet Centre: http://www.saferinternet.org.uk
- Internet Matters (Helping parents keep their children safe online): https://www.internetmatters.org
- The Parent Zone: https://parentzone.org.uk
- ParentINFO: http://parentinfo.org

Updated links can also be found on the Alec Hunter Academy website

Student Internet and E-mail Access

- All Student internet access via school computers will be supervised. This means there will be a member of staff in the room who is aware that the students are accessing the internet. The use of RM Tutor allows for monitoring of student computer access.
- Inappropriate access to on-line material – internet access is filtered through our Internet Service Provider (ISP). This is not infallible but students who have deliberately tried to access filtered material or to bypass the filtering service will have their internet access suspended.
- The school e-mail service may be used for personal use, however in accordance with the guidance on language and e-mail use.
- Misuse may result in suspension of internet access for a fixed period, and in serious cases indefinitely.
- Students should not access website guestbooks, forums or chatrooms due to the unregulated nature of the content, unless there is a clear educational value and a member of staff is aware and directing the activity.
- Students are able to use their personal mobile phones during break and lunchtime but only when in the allocated phone room. The school does not provide the students with wi-fi facilities. If a student chooses to use personal data on a mobile phone to access the internet, then the same expectations are in place with regards to what they can/can't access.

Guidance on Unacceptable Usage of Alec Hunter Academy Network

Personal Safety

- Students must not send or publish personal contact information about themselves or other people – this includes home address, mobile telephone number, school address, etc – other than for official purposes e.g. college applications.

- Students must not access or contribute to on-line forums, chat rooms or comment boards associated with web sites, even if those websites are not filtered e.g. BBC comments pages.
- Students must promptly disclose to a member of staff any message they receive that is inappropriate or makes them feel uncomfortable.

Illegal Activity

- Users must not attempt to gain unauthorised access to the school's network or go beyond their authorised access. This includes trying to log-on through another person's account or accessing another person's files. These action are illegal even if only for the purpose of "browsing".
- Users must not attempt to bypass the internet filtering system. Such attempts may results in a permanent suspension of internet privileges and disciplinary action.
- Users must not make deliberate attempts to disrupt the computer system or destroy data by spreading computer viruses or by any other means. These actions are illegal.
- Any material that the school believes is illegal will be referred to the appropriate authorities.

System Security

- Users are responsible for their individual user area and should take all reasonable precautions to prevent others from being able to use it. Under no circumstances should users let anyone else know their password.
- Users must immediately notify a system administrator or IT teacher if they have identified a possible security problem. Users should not go looking for security problems because this could be construed as an illegal attempt to gain access.
- Users should take adequate measures to protect the network from inadvertent damage, such as the spread of computer viruses. Unchecked disks and USB flash/pen drives must not be used and e-mail attachments that are suspect or from unknown sources should not be opened.
- Users must download computer programs or files from the internet without permissions from a member of staff (students) or the Network Manager (Staff).
- Users must not try to load programs onto the school's network or attempt to run programs that are not accessible through their user's standard privileges.

Inappropriate Language

- Restrictions against inappropriate language apply to public and private e-mail messages, file names, the content of files and material posted on Web pages.
- Inappropriate language includes obscene, profane, lewd, vulgar, rude, inflammatory, threatening, swearing or disrespectful language.

Misuse of Communication Services

This section applies primarily to email. However, it also applies to any other form of communication which takes place across the school network, or on the school site via personal mobile phones:

- Users must not distribute information that could cause damage or a danger of disruption;
- Users must not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If a user is told by someone to stop sending messages, then they must stop;

- Users must not knowingly or recklessly distribute false or defamatory information about a person or organisation;
- Students must not forward a message that was sent privately without the permission of the person who sent the message;
- Students must not e-mail private information about another person;
- Users must not distribute chain letters or engage in "spamming". Spamming is sending an annoying or unnecessary message to a large number of people;
- Students must not use any other online communication services except email in lessons unless they have gained permission from the member of staff taking the lesson.

Misuse of Resources

- There are only a limited amount of computers available outside of lesson time. Priority will be given to those students who need access for educational or careers purposes and students given access must use the internet only for those purposes.
- All users must avoid unnecessary printing.
- Accessing and playing games on the internet is not permitted at any point.
- For copyright reasons, students must not use their network area to store executable files (programs) or non-educational multi-media files, such as MP3s or video clips.
- Shared areas on the school's network are for transferring files and all users are responsible for their removal when they are no longer needed. If any users place an inappropriate file in a shared area, disciplinary action may result.
- Listening to on-line radio broadcasts or watching website video clips online slows the network. Unless this is for an educational reason authorised by a member of staff, this is not permitted.

Monitoring of the Network

- For safeguarding reasons, all users should not expect privacy relating to their use of the network. Any and all communication and data stored on, or sent via, the school network may be monitored by automated or manual systems.
- Monitoring may include communication sent over the school's wi-fi service from personal devices which have connected to that service.
- Routine maintenance and monitoring of files stored on the school's network may lead to discovery that users have violated this policy or the law.
- Routine monitoring of user logs, user files and the screens of users using the internet may lead to discovery that users have violated this Policy or the law.
- An individual search will be conducted if there is a reasonable suspicion that this Policy has been violated. The investigation will be reasonable and related to the suspected violation.
- Alec Hunter Academy has implemented a new monitoring solution in August 2015 called RM Tutor to ensure student safety while on the school site. RM Tutor allows staff to view what students are doing on the computer live during lessons and control the content available to them in the classroom environment.
- Securus contains an editable keyword library which picks up inappropriate or extremist language and logs it with a screenshot, timestamp and student user information. The incident is then brought to the attention of staff.

Policy Violations

- Alec Hunter Academy will co-operate fully with local or government officials in any investigation related to any illegal activities conducted through the school's network.
- Misuse of the internet or email may result in access to these facilities being suspended or removed. Further disciplinary action may also result for any user found to be in breach of this code.

Personal Responsibility

All users should be aware of the following:

- All user actions on the school's network may be logged. This information may include the workstation used, the time logged on for, the websites accessed, what software was used and any printing done.
- These logs may be used to track specific actions by users or workstations at any given time.
- All users are responsible for the contents of their user area. If obscene or inappropriate files are found by routine scans, then disciplinary action may result.
- Where students have accessed or stored inappropriate material, details and/or printouts of such material may be communicated to parents/guardians and suitable sanctions will be imposed by the school.

Personal/Portable Technology

- Students may not bring portable computing devices (tablets/Ipads) into school unless they are to be used in the context of a special educational need.
- Mobile phones and personal music players may be brought into school but must be switched off and not used during lessons. Please also note that mobile phones are not allowed to be used anywhere inside of the school buildings except in the mobile phone room at break and lunchtime.
- Mobile phone cameras should not be used at any time.
- The school cannot accept any liability for the loss or damage of any personal devices brought into school by students.
- A student's device may be confiscated and parents required to collect the device from school if a student fails to follow a teacher's instructions regarding its use. The procedure following confiscation of a device can be found in the school's Mobile Phone Policy.
- The school recognises the potential conflict between the student's right to privacy and the need to investigate incidences of misuse involving personal devices. Parental consent will therefore be sought, where possible, before any examination of such devices is undertaken by school staff. In cases where criminal activity is suspected, no examination will be made by school staff and all devices will be handed to the police for investigation.
- New and emerging personal technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

The Law

While this policy outlines expectation on usage, some of these expectations are a legal requirement and violation of the policy could lead to prosecution.

Communications Act 2003 (Section 127)
Sending by means of internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the internet for the purpose of causing annoyance, inconvenience or needles anxiety is guilty of an offence, liable on conviction to imprisonment.

Malicious Communication Act 1988 (Section 1)
This legislation makes it a criminal offence to send an electronic message that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purposed was to cause a recipient to suffer distress or anxiety.

Protection from Harassment Act 1997
A person must not pursue a course of conduct which amounts to the harassment of another, and which they know or ought to know amounts to the harassment of another.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against them, is guilty of an offence if they know or ought to know that their course of conduct will cause the other to fear on each of those occasions.

Computer Misuse Act 1990
This legislation makes it a criminal offence to gain unauthorised access to another students area even if you don't change/delete any information in the area.