Braunton Academy
Aspire & Achieve

Policy 6.28
Mar 2019

Online Safety Policy

1. Introduction and Overview

The purpose of this policy is to:

- Outline the guiding principles for all members of the Academy community regarding the use of ICT.
- Safeguard and protect the students and staff and help them to work safely and responsibly with the internet and other communication technologies.
- Set clear expectations of behaviour relating to responsible use of the internet for educational, personal or recreational use.
- Establish clear reporting mechanisms to deal with online abuse such as bullying that are cross referenced with other Academy policies.
- Ensure that all members of the Academy community know that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

Scope of the policy
This policy applies to all members of Academy community - staff, students, volunteers, parents and carers, visitors, community users - who have access to and are users of Academy's ICT systems.

Communication of the policy
The policy will be communicated to the Academy community in the following ways:

- Displayed on the Academy website, and available in the staffroom and classrooms.
- Included as part of the induction pack for new staff.
- Acceptable use agreements discussed with and signed by students at the start of each year. Communicated to parents who sign each year.
- Acceptable use agreements to be issued to whole Academy community, usually on entry to the Academy – and read and signed annually by all staff and Governors.
- Acceptable use agreements to be held in student and personnel files.

Responding to complaints

- The Academy will take all reasonable precautions to ensure internet safety. However, it is not possible to guarantee that unsuitable material will never appear on an Academy computer or mobile device. The Academy cannot

accept liability for material accessed, or any consequences of internet access.
- Staff and students are informed of the possible sanctions related to misuse of technology and these are outlined in the Behaviour 4 Learning Policy.
- Our Online Safety Coordinator is the first point of contact for any complaint. Any complaint about staff misuse will be referred to the Principal.
- Complaints that relate to online bullying will be dealt with in line with our Anti-Bullying Policy. Complaints related to child protection are dealt with in line with the Academy child protection procedures.

Review and Monitoring
Online safety is integral to other Academy policies including the Child Protection Policy, Anti-Bullying Policy and Behaviour For Learning Policy.

The Academy's Online Safety Officer is responsible for writing, reviewing and updating the policy. The policy will be reviewed annually or more frequently in response to changing technology and internet safety issues in the Academy.

This policy has been developed in consultation with the Academy's ICT Strategic Group, and approved by the Senior Leadership Team and Board of Governors. All stakeholders will be informed of any updates or amendments to it as it applies to them

2. Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the Academy

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors Safeguarding Portfolio receiving regular information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of Online Safety Governor

Principal

- The Principal has a duty of care for ensuring the safety (including online safety) of members of the Academy community, though the day to day responsibility for online safety will be delegated to the *Online Safety Officer*
- The Principal and Deputy should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (see flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse" and relevant *Local Authority / MAT / other relevant body* disciplinary procedures
- The Principal is responsible for ensuring that the Online Safety Officer and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

- The Principal will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles. This is done with regular 1 to 1 meetings between the Online Safety Officer and the Principal.

Online Safety Officer

- leads the Online Safety Group (part of the IT strategic committee]
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the Academy online safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with IT support staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments. This is done via SIMS reports.
- meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- attends relevant meetings of the Safeguarding Portfolio Group
- reports regularly to Senior Leadership Team

Network Manager

The Network Manager is responsible for ensuring:

- that the Academy's technical infrastructure is secure and is not open to misuse or malicious attack
- that the Academy meets required online safety technical requirements and any other relevant body Online Safety Policy
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- that the use of the network / internet / Learning Platform / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Principal / Online Safety Officer for investigation
- that monitoring software / systems are implemented and updated as agreed in Academy policies

Other stakeholders roles and responsibilities are outlined in the relevant acceptable use agreements read and signed annually.

Community Users

Community Users or visitors wishing to use the Academy IT systems or access the Internet need to email support@braunton.academy before the visit. Support will email an electronic form to be completed. [See appendix]. Where community

users/visitors are bringing in a memory stick to use, then it will need to be scanned by support before use. It is the responsibility of staff hosting visitors who need to advise visitors about the relevant protocols

3. Education and Curriculum

Student internet safety curriculum

The Academy has a clear, progressive online safety education programme primarily as part of the Computing curriculum / PSHE curriculum but referenced in all areas of Academy life. It covers a range of skills and behaviours appropriate to students' ages and experience, including:

- Digital literacy.
- Acceptable online behaviour.
- Understanding of online risks.
- Privacy and security.
- Reporting concerns.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.

Staff and governor training

The Academy will ensure that:

- Staff understand the requirements of the Data Protection Act in terms of sending and receiving sensitive personal information.
- Regular training is available to staff on online safety issues and the Academy's internet safety education programme.
- Information and guidance on the Safeguarding policy and the Academy's Acceptable Use Policy is provided to all new staff and governors.

Parent engagement

The Academy recognises the important role parents and carers have in ensuring children and young people are safe, responsible and can flourish online. To support parents to understand online risks and the work of the Academy in this area we will provide:

- Acceptable Use Agreements to all new parents.
- Regular, up to date information in newsletters and on the website and social media, particularly in response to emerging trends.
- Face to face sessions in Academy.
- Opportunities to share in their children's internet safety learning (eg assemblies, performances).
- Support and advice on online safety for their children outside of Academy.
- Signposting to further resources and websites.

4. Conduct and Incident management

Conduct

All users are responsible for using the Academy ICT systems in line with the Acceptable Use Policy they have signed. They should understand the consequences of misuse or access to inappropriate materials.

All members of the Academy community should know that this policy also covers their online activity outside of Academy if it relates to their membership of the Academy.

Parents and carers will be asked to give consent for their children to use the internet and other technologies in Academy, by signing an Acceptable Use Agreement. They will also be given clear information about the sanctions that might result from misuse.

Incident Management

All members of the Academy community understand they have a responsibility to report issues and are confident that anything raised will be handled quickly and sensitively, in line with the Academy's Misuse Plan. The Academy actively seeks advice and support from external agencies in handling internet safety issues. Parents and carers will be informed of any internet safety incidents relating to their own children.

5. Managing the ICT infrastructure

The Academy is responsible for ensuring that the Academy infrastructure is as safe and secure as is reasonably possible and that related policies and procedures are implemented. It will also ensure that the relevant people will be effective in carrying out their internet safety responsibilities with regards to the ICT infrastructure.

- The technical systems will be managed in ways that ensure that the Academy meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of the Academy's technical systems.
- All users will have clearly defined access rights to the technical systems and Academy owned devices.
- All users will be provided with a username and secure password. Users will be responsible for the security of their username and password.
- The administrator passwords for the Academy ICT system, used by the Network Manager is also available to the Principal and kept in a secure place.
- Internet access is filtered for all users. Illegal content (child sexual abuse images). Extreme and terrorist material is also filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- The Academy allows different filtering levels for different ages / stages and different groups of users – staff / students.
- The Academy regularly monitors and records the activity of users on the Academy technical systems and users are made aware of this in the Acceptable Use Agreement.
- There is a reporting system in place for users to report any technical incident or security breach.
- Security measures are in place protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the Academy systems and data. These are tested regularly. The Academy infrastructure and individual workstations are protected by up to date virus software. Servers, wireless systems and cabling must be kept securely located and physical access restricted.
- Personal data cannot be sent over the internet or taken off the Academy site unless safely encrypted or otherwise secured.

Social Media

The Academy has a Social Media Policy that covers the management of Academy accounts and set out guidelines for staff personal use of social media.

6. Data

The Academy has a GDPR Data Protection and Document Retention and Handling Policy that is regularly reviewed and updated. This includes information on the transfer of sensitive data, the responsibilities of the Data Protection Officer, and the storage and access of data.

7. Equipment and Digital Content

Personal mobile phones and mobile devices

Personal mobile phones and mobile devices brought in to Academy are the responsibility of the device owner. The Academy accepts no responsibility for the loss, theft or damage of personal mobile phones or mobile devices.

Student Use

The Academy strongly advises that student mobile phones should not be brought into Academy.

Student mobile phones must be turned off / placed on silent and stored out of sight in Academy. They must remain turned off and out of sight until the end of the day. Mobile phones will not be used during lessons or formal Academy time unless with consent from a member of staff after permission from the Internet Safety Officer/Principal.

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

Authorised staff can search student's electronic devices if they have good reason to think that the device has been or could be used to cause harm, disrupt teaching or break Academy rules. Any search will be carried out in line with the Academy's Search Procedures – Electronic Devices.

Staff Use

Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity, except in exceptional circumstances

Staff devices, including mobile phones and cameras, must be noted in Academy – name, make & model, serial number. Any permitted images or files taken in Academy must be downloaded from the device and deleted in Academy before the end of the day.

Mobile phones and other devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or other personal devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team.

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

Where staff are required to use a mobile phone for Academy duties – e.g. in case of emergency during off-site activities, or for contacting students or parents - then an Academy mobile phone will be provided. In an emergency where staff do not have access to an Academy device, they should use their own device and hide their own number (by dialling 141 first).

Digital images and video

We will seek permission from parents and carers for the use of digital photographs or video involving their child as part of the Use of Digital and Video Images Agreement when their child joins the Academy.

We do not identify pupils in online photographic materials or include the full names of students in the credits of any published Academy produced video.

If specific student photos (not group photos) are used on the Academy website or prospectus we will obtain individual parental or student permission for its use.

Students are taught to think carefully about placing any personal photos on social media sites. The importance of privacy settings as a tool to safeguard their personal information is included in internet safety education. They are also taught that they should not post images or videos of others without their permission.

Students understand the risks associated with sharing images that reveal the identity of others and their location, such as house number, street name or Academy.

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.