

HAZELEY ACADEMY



Online Safety Policy

Scope of the Policy

This policy applies to all members of the Academy community (including staff, students, volunteers, parents/carers, visitors, community users) who have access to and are users of Academy ICT systems, both in and out of the Academy.

The Education and Inspections Act 2006 empowers Headteachers/Principals to such extent as is reasonable, to regulate the behaviour of students when they are off the Academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other Online Safety incidents covered by this policy, which may take place outside of the Academy, but is linked to membership of the Academy. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. The Academy will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate Online Safety behaviour that take place out of school.

Roles and Responsibilities

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

Board of Directors:

Directors 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 Governing Body by receiving regular information about online safety incidents and monitoring reports, as part of Safeguarding reports made to the board by the DSL. A member of the Board has taken on the role of Online Safety Director, combined with the role of the Child Protection/Safeguarding Governor).

Principal and Senior Leaders:

- The Principal has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the DSL for safeguarding matters and the Network Manager and their team for the technical aspects.
- The Principal and Senior Leaders are responsible for ensuring that the DSL and/or their team and the Network Manager and their team 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/ Senior Leaders 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.
- The Senior Leadership Team/Senior Management Team will receive regular monitoring reports from the DSL/Network Manager

Network Manager/Technical staff:

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.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the internet filtering, is applied and updated on a regular basis preventing unwanted access to sites that can be in breach of the IT acceptable usage policy. Its implementation is not the sole responsibility of any single person
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the *network/internet/remote access/email* is regularly monitored in order that any misuse/attempted misuse can be reported via CPOMS to the DSL for investigation/action/sanction
- that monitoring software/systems are implemented and updated as agreed in Academy policies.

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current Academy Online Safety Policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy/Agreement (AUP)
- they report any suspected misuse or problem to the DSL via CPOMS for investigation/action/sanction
- all digital communications with students /parents/carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- students understand and follow the Online Safety Policy and acceptable use policies
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Designated Safeguarding Lead (including role as Online Safety Co-ordinator)

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school 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 the Local Authority as appropriate
- liaises with school technical staff
- receives reports of online safety incidents, to be recorded on CPOMS, to inform future online safety developments,
- reports regularly to Senior Leadership Team

Should be trained in Online Safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- cyber-bullying

Students:

- are responsible for using the Academy digital technology systems in accordance with the Student/Pupil Acceptable Use Agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the Academy's Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The Academy will take every opportunity to help parents understand these issues *through parents' evenings, blogs, letters, website and information about national/local online safety campaigns/literature*. Parents and carers will be encouraged to support the Academy in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to on-line student/pupil records
- their children's personal devices in the Academy

Policy Statements

Education – Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating *students* to take a responsible approach. The education of *students* in online safety is therefore an essential part of the school's/Academy's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience. 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.
- The Counter Terrorism and Securities Act 2015 require schools to ensure that children are safe from terrorist and extremist material on the internet.
- Students should be helped to understand the need for the Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside Academy.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

Education – Parents/Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The Academy will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, website, School comms texts and emails
- Parents/Carers evenings/sessions
- High profile events/campaigns e.g. Safer Internet Day
- Reference to the relevant web sites/publications e.g. [swgfl.org.uk](http://www.swgfl.org.uk), www.saferinternet.org.uk/ <http://www.childnet.com/parents-and-carers>

Education – Staff/Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the Academy Online Safety Policy and Acceptable Use Agreements.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Training – Governors/Directors

Governors/Directors should take part in online safety training/awareness sessions. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/National Governors Association/or other relevant organisation (e.g. SWGfL).
- Participation in Academy training/information sessions for staff or parents (this may include attendance at assemblies/lessons).

Technical – infrastructure/equipment, filtering and monitoring

The Academy will be responsible for ensuring that the Academy infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

Academy 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 Academy technical systems

- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to Academy technical systems and devices.
- All users will be provided with a username and secure password by IT Support who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password every 90 days.
- The IT manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is 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
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet. Nb. additional duties for schools/academies under the Counter Terrorism and Securities Act 2015 which requires schools/academies to ensure that children are safe from terrorist and extremist material on the internet.
- The Academy has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different ages/stages and different groups of users – staff /students etc)
- Academy technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement. We have an education specific proxy server and also have impero running on the network to monitor and protect the network.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed). As per the AUP, all users need to report incidents to IT support, preferably via email but if not in person.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software. We have the up to date Anti-Virus software and definitions and also run an education specific proxy and email filter (Smoothwall).

- An agreed procedure is in place for the provision of temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors) onto the school systems. We have a guest account that we supply with visitors and the password is rotated periodically. This user also has restricted access to the internet and our network.
- An agreed procedure is in place regarding the extent of personal use that users (staff/Students/ community users) and their family members are allowed on school devices that may be used out of school. School policy is in place to ensure that the designated owner of the device is responsible for its use external to the Academy.
- An agreed procedure is in place that allows staff to/forbids staff from downloading executable files and installing programmes on school devices. We have antivirus software running on all clients and servers, and the proxy protecting downloads.
- An agreed procedure is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured. We have remote access for all staff that need to access our systems remotely so there is no need for staff to store or send any data off site.

Mobile Technologies incl. Bring your own device/Bring your own technology

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school’s wireless network. The device then has access to the wider internet which may include the school’s learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use mobile/personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school policies including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school’s Online Safety education programme.

- The school Acceptable Use Agreements for staff, pupils/students and parents/carers will give consideration to the use of mobile technologies

Use of digital and video images

Staff use of digital and video images is covered in detail in the Staff Code of Conduct document.

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- Written permission from parents or carers will be obtained before photographs of students are published on the school website/social media/local press
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at Academy events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other *students* in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school Academy policies concerning the sharing, distribution and publication of those images.
- Care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the Academy into disrepute.
- Students must not take, use, share, publish or distribute images of others during the school day, or whilst on a school activity, without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities. With any incident, the academy Safeguarding procedures will be followed as appropriate.

Academy Actions & Sanctions

It is more likely that the Academy will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures.

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 for responding to online safety incidents and report immediately to the police.

