The Quest Academy

e-Safety Policy

Purpose

The Quest Academy online safety policy aims to create an environment where students, staff, parents, governors and the wider Academy community work together to inform each other of ways to use the Internet responsibly, safely and positively.

Internet technology helps students learn creatively and effectively and encourages collaborative learning and the sharing of good practice amongst all Academy stakeholders. The e-Safety policy encourages appropriate and safe conduct and behaviour when achieving this. It is underpinned by the Academy's Acceptable Use Policy.

The Academy will make reasonable use of relevant legislation and guidelines to inform positive behaviour regarding IT and Internet usage both on and off the Academy site. This will include imposing sanctions for inappropriate behaviour in line with the regulation of student behaviour under the Education and Inspections Act 2006.

Students, staff and all other users of school-related technologies will work together to agree standards and expectations relating to usage in order to promote and ensure good behaviour. It is intended that the positive effects of the policy will be seen online and offline, in the Academy and at home and, ultimately, beyond school and into the workplace.

The e-Safety policy and Acceptable Use Policy will be reviewed at, or prior to, the start of each academic year and promptly in the following instances:

- Serious and/or frequent breaches of the Acceptable Internet Use Policy or in the light of e-safety incidents.
- New guidance by government/local authority/safeguarding authorities.
- Significant changes in technology as used by the Academy or students in the wider community.
- E-safety incidents in the community or local schools which might impact on the Academy's community.
- Advice from the police and/or local safeguarding children partners.

The Quest Academy aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

This policy complies with our funding agreement and articles of association.

Roles and responsibilities

The governing board

The governing board has overall responsibility for monitoring this policy and holding the Principal to account for its implementation.

This governor will:

- Provide and evidence a link between the Academy, governors and parents.
- Liaise with the e-safety officer/coordinator with regard to reports on e-safety effectiveness, incidents, monitoring, evaluation and developing and maintaining links with local stakeholders and the wider school community. Complete an audit of Governor IT competence, relevant outside experience and qualifications to identify training needs and create a schedule and development plan.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL).

The governing body will appoint a designated governor who oversees online safety.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the Academy's ICT systems and the internet.

The Senior Leadership Team

The Academy's senior leadership is responsible for:

- Determining, evaluating and reviewing e-safety policies to encompass teaching and learning, use of Academy IT equipment and facilities by students, staff and visitors.
- Agreeing criteria for the acceptable use by students, Academy staff and governors of Internet capable equipment for school-related purposes or in situations which will impact on the reputation of the Academy, and/or on Academy premises.

They will ensure that:

- There is a cycle of evaluation and review based on new initiatives and partnership discussion with stakeholders and outside organisations, technological and Internet developments, current government guidance and school-related e-safety incidents.

- Good practice is implemented within the teaching curriculum and wider pastoral curriculum.
- Inset development is identified and provided for staff and governors and guidance provided to parents, students and local partnerships.
- Management is encouraged to be aspirational and innovative in developing strategies for, and a calendar of, e-safety provision which will deliver measurable success and clearly state e-safety targets with success criteria on the Academy development plan.

The Designated Safeguarding Lead

Details of the Academy's Designated Safeguarding Lead (DSL) and Deputy Designated Safeguarding Leads (DDSL) are set out in our safeguarding and child protection policy. The DSL also acts as the Academy's E-Safety Officer.

The DSL takes lead responsibility for online safety in the Academy, in particular:

- Supporting the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the Academy
- Working with the Principal, Director of IT, IT Systems Manager and other staff, as necessary, to address any online safety issues or incidents.
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the Academy's behaviour and anti-bullying policy.
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in the Academy to the Principal and/or governing board.

This list is not intended to be exhaustive.

The Director of IT

The Director of IT is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep students safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the Academy's IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are reported to the DSL and dealt with appropriately in line with this policy

This list is not intended to be exhaustive.

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the Academy's IT systems and the internet, and ensuring that students follow the Academy's terms on acceptable use.

- Working with the DSL to ensure that any online safety incidents are reported and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the Academy's behaviour policy.

This list is not intended to be exhaustive.

Parents

Parents are expected to:

- Notify a member of staff or the Principal of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the Academy's IT systems and internet.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

Visitors and members of the community

Visitors and members of the community who use the Academy's IT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

Students

Students are required to:

- Use Academy Internet and computer systems in agreement with the terms specified in the Academy's Acceptable Use Policies.
- Understand that the policies also cover the use of personal items such as phones and their Internet use out of school on social networking sites such as Instagram if it impacts on the Academy and/or its staff and students in terms of cyber bullying, reputation, YPSI or illegal activities.
- Be aware of how to report e-safety incidents in school, and how to use external reporting facilities, such as the Click CEOP button or Childline number.

Educating students about online safety

Students will be taught about online safety as part of the curriculum.

In Key Stage 3, students will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns.

Students in Key Stage 4 will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns.

The safe use of social media and the internet will also be covered in other subjects where relevant.

The Academy will use assemblies to raise students' awareness of the dangers that can be encountered online and may also invite speakers to talk to students about this.

Educating parents about online safety

The Academy will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

Online safety will also be covered during parents' information evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the DSL.

Concerns or queries about this policy can be raised with any member of the Academy's leadership team**.**

Cyber-bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the Academy's behaviour policy.)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The Academy will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form tutors will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the Academy will follow the processes set out in the Academy behaviour policy. Where illegal, inappropriate or harmful material has been spread among students, the Academy will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Examining electronic devices

Academy staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on students' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the Academy rules
- If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the Senior Leadership Team to decide whether they should:
  - Delete that material, or
  - Retain it as evidence (of a criminal offence or a breach of Academy discipline), and/or
  - Report it to the police.

Any searching of students will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the Academy complaints procedure.

Acceptable use of the internet in school

All students, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the Academy's IT systems and the internet. Visitors will be expected to read and agree to the Academy's terms on acceptable use if relevant.

Use of the Academy's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements.

Students using mobile devices in the Academy

Students may have mobile devices on their person, but must not use them when in school.

Any use of mobile devices in the Academy by students may trigger disciplinary action in line with the Academy behaviour policy, which may result in the confiscation of their device.

Staff using work devices outside of the Academy

Staff members using a work device outside of the Academy must not install any unauthorised software on the device and must not use the device in any way which would violate the Academy's terms of acceptable use.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside of the Academy. Any USB devices containing data relating to the Academy must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the Director of IT or one of the senior IT Support Team.

Work devices must be used solely for work activities.

How the Academy will respond to issues of misuse

Where a student misuses the Academy's IT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the Academy's IT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The Academy will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Responding to e-Safety concerns

Typical e-safety incidents perpetrated by students, staff, parents, governors, contractors and others include:

- Finding illegal material on the network which could raise a child protection issue.
- Going on the Internet during lesson time for reasons not related to the lesson.
- Bypassing the Academy's filtering system.
- Viewing pornographic material.
- Using a mobile phone or other digital device in a lesson.
- Using social media or email during a lesson.
- Cyber-bullying.
- Writing malicious comments about the Academy or bringing the Academy name into disrepute (whether in school time or not).
- Sharing usernames and passwords.
- Deleting someone else's work or unauthorised deletion of Academy files.
- Trying to hack or hacking into another person's account, Academy databases, Academy website, Academy emails or online fraud using the Academy's network.
- Uploading or downloading files using the Academy's network.

- Copyright infringement of text, software or media.

The Academy's approach to dealing with an incident and applying sanctions aims to demonstrate the correlation between procedures and sanctions for students and procedures and sanctions for staff.

The reporting process and sanctions will depend on:

- Whether an illegal act has taken place
- Whether there is a safeguarding issue (in which case we will follow the guidelines in our Safeguarding Policy)
- The nature and severity of the incident
- Whether the person has previously had sanctions for a similar incident.

Note that under The Education and Inspections Act 2006 headteachers have the power "to such an extent as is reasonable" to regulate the conduct of students off site. Also, staff can confiscate mobile phones if they cause a disturbance in class in breach of the Academy's Behaviour Policy.

These general principles apply in dealing with an incident:

- Evidence should be collected and preserved – this may involve assistance from IT Systems Manager.
- Incident reports will be completed and submitted to the DSL.
- Appropriate disciplinary action/sanctions will be taken following the Academy's procedures.
- Parents/carers may be informed.

The police and/or other relevant agencies will be notified in certain circumstances, including:

- if an indecent image has been taken
- in the case of cyber-bullying
- An incident of hacking or online fraud

Offending content will be removed if possible and a review of security will be carried out where relevant.

If a website is hosted in the USA, or operates under US law, then the Digital Millennium Copyright Act will apply for copyright infringement. This is very useful when seeking to remove photographs and other material which has been copied onto a site such as Facebook and Twitter.

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and Deputy DSL's will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. These are recorded and reported on the Academy’s online safeguarding system, CPOMS.

This policy will be reviewed annually by the DSL. At every review, the policy will be shared with the governing board.

Links with other policies

This online safety policy is linked to our:

- Safeguarding & Child Protection Policy
- ICT Acceptable Use Policy for Students - E Safety Rules
- Student Discipline Including Anti Bullying Behaviour Policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

Trust Policy

This Academy e-Safety policy works in conjunction with The Collegiate Trust’s ICT policy which can be found here: ICT-Policy-2020.pdf (tct-academies.org).