Castle View Academy
The best in everyone™
Part of United Learning

E-Safety Policy

Background/Rationale

New technologies have become integral to the lives of our children and young people in today's society, both within the Academy and in their lives outside the Academy.

The internet and other digital and information technologies are powerful tools which open up new opportunities for everyone. Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in the Academy are bound. A school E-Safety Policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the stakeholders in a child's education from the Principal and Governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the students themselves. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote student achievement.

However, the use of these new technologies can put young people at risk within and outside the Academy. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person

Many of these risks reflect situations in the off-line world and it is essential that this E-Safety Policy is used in conjunction with other Academy Policies, including the Acceptable Use Policy, Behaviour for Learning Policy and Safeguarding & Child Protection Policy.

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

Castle View Academy must demonstrate that they have provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The E-Safety Policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents/carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

The Academy will monitor the impact of the policy using:

Reviewed	June 2019
Next review	June 2021

- Logs of reported incidents
- Internet provider monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys / questionnaires – students; parents/cares; staff

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers, 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 e-safety incidents covered by this policy, which may take place outside of the Academy, but is linked to membership of the Academy. The Academy will deal with such incidents within this policy and associated Behaviour for Learning and Anti-Bullying Policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of the Academy.

Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the Academy:

Governors:

- Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out through regular reporting to Governor Committee by the Designated Senior Person for Safeguarding and Child Protection.

Principal / Senior Leaders:

- The Principal is responsible for ensuring the safety (including e-safety) of members of the Academy community, though the day to day responsibility for e-safety will be delegated to the Designated Senior Person for Safeguarding and Child Protection
- The Designated Senior Person for Safeguarding and Child Protection will liaise with the Academy Network manager and ICT staff in order to monitor all aspects of e-safety
- The Principal and Designated Senior Person for Safeguarding and Child Protection will set out procedures to be followed in the event of a serious e-safety allegation being made against a member of staff in line with the Academy Acceptable Use Policy and Safeguarding Policy

The Designated Senior Person for Safeguarding and Child Protection will also:

- Liaise with relevant staff
- Have a leading role in establishing and reviewing the Academy E-Safety Policy and other relevant documents
- Ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- Provide training and advice for staff
- Liaise with the Academy ICT teaching and technical staff
- Receive reports of e-safety incidents and ensure a log of incidents is kept to inform future e-safety developments
- Meet regularly with the Safeguarding Governors to discuss current issues, review incident logs and filtering / change control logs

- Attend relevant Governor meetings

Network Manager / Technical Staff

The Network Manager / ICT Support Staff are responsible for ensuring:

- That the Academy ICT infrastructure is secure and is not open to misuse or malicious attack
- That the Academy meet appropriate e-safety technical requirements to fulfil the Acceptable Use Policy
- That users may only access the Academy networks through a properly enforced password protection system, in which passwords are regularly changed
- That the internet provider is informed of issues relating to the filtering they apply
- That they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- That the use of the network / remote access / email is regularly monitored in order that any misuse or attempted misuse can be reported to the Designated Senior Person for Safeguarding and Child Protection for investigation and action
- That monitoring software / systems are implemented and updated as agreed in Academy policies

Teaching and Support Staff

Teaching and Support Staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current Academy e-safety policy and practices
- They have read, understood and signed off the Academy Staff Acceptable Use Policy
- They report any suspected misuse or problem to the Designated Senior Person for Safeguarding and Child Protection or Network Manager as appropriate
- Digital communications with students are on a professional level and only carried out using official Academy systems
- E-safety issues are embedded in all aspects of the curriculum and other Academy activities
- Students understand and follow the Academy E-Safety and Acceptable Use Policy
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extra-curricular and extended Academy activities
- They are aware of e-safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current Academy 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

Students

- Are responsible for using the Academy ICT systems in accordance with the Student Acceptable Use Policy, which they will be expected to sign before being given access to Academy systems
- 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 Academy policies on the use of mobile phones, digital cameras and hand-held devices. They should also know and understand Academy policies on the taking / use of images and on cyber-bullying
- Should understand the importance of adopting good e-safety practice when using digital technologies out of the Academy and realise that the Academy E-Safety Policy covers their actions whilst outside of the Academy, if related to their membership of the Academy

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. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The Academy will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / information about national/ local e-safety campaigns / literature.

Parents and carers will be responsible for:

- Endorsing (by signature) the Student Acceptable Use Policy
- Accessing the Academy website /student records in accordance with the relevant Academy Acceptable Use Policy

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 e-safety is therefore an essential part of the Academy e-safety provision. Children and young people need the help and support of the Academy to recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

- Through a planned e-safety programme through ICT / SMSC / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in and outside school
- Through key e-safety messages reinforced as part of a planned programme of assemblies
- 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 helped to understand the need for them to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside of the Academy
- Students will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Staff should act as good role models in their use of ICT, the internet and mobile devices

Many parents and carers have only a limited understanding of e-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 experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide" – Byron Report.

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

- Letters, newsletters, website
- Parents consultation and information evenings

All staff will receive e-safety training in order to understand their responsibilities, as outlined in the policy. Training may take the format of:

- A planned programme of formal e-safety training made available to staff following an audit of the training needs. It is expected that some staff will identify e-safety as a training need within the performance management process
- All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the Academy E-Safety Policy and Acceptable Use Policy
- Regular updates will be provided to all staff through ICT staff or the Designated Senior Person for Safeguarding and Child Protection

Governors will be invited to take part in e-safety training through:

- Attendance at training provided by the Local Authority / National Governors Association or other relevant organisation
- Participation in Academy training / information sessions for staff or parents

Curriculum

E-Safety should be a focus in all areas of the curriculum and should reinforce e-safety messages in the use of ICT across the curriculum

- In lessons where internet use is pre-planned, it is best practice that 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
- Where students are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager 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
- 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

Use of digital and video images – photographic, video

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 and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The Academy will inform and educate users about these risks and will implement systems to reduce the likelihood of the potential for harm.

When using digital images, staff should inform and educate students about the rules and risks associated with the taking, use, sharing, publication and distribution of images.

- Staff are allowed to take digital / video images to support educational aims, but must follow Images of Children protocol concerning the sharing, distribution and publication of those images. Those images should only be taken on Academy equipment, the personal equipment of staff should not be used for such purposes
- 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 of the Academy into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with Images of Children protocol
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of students are published on the Academy website

Data Protection

Personal data will be recorded, processed, transferred and made available according to the latest GDPR regulations which state that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection

Staff must ensure that they always:

- Take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly 'logged-off' at the end of any session in which they are using personal data
- Transfer data using encryption and secure password protected devices

When personal data is stored on any portable computer system, USB stick or any other removable media:

- The data must be encrypted, and password protected
- The device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- The device must offer approved virus and malware checking software
- The data must be securely deleted from the device, in line with Academy policy once it has been transferred or its use is complete

Communications

When using communication technologies, the Academy will consider the following as good practice:

- The official Academy email service may be regarded as safe and secure and is monitored
- Users need to be aware that email communications are monitored
- Users must immediately report the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email
- Any digital communication between staff and students or parents / carers (email, chat, Facebook etc.) must be professional in tone and content. These communications may only take place on official (monitored) Academy systems. Personal email addresses, text messaging or public chat programmes must not be used for these communications
- Students should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material
- Personal information should not be posted on the Academy website and only official email addresses should be used to identify members of staff

Responding to incidents of misuse

It is hoped that all members of the Academy community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless, irresponsible or, very rarely, deliberate misuse.
Examples of misuse include:

- Child sexual abuse images
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Other criminal conduct, activity or materials

Incidents of misuse will be dealt with in line with either the LA or United Learning Safeguarding and Disciplinary procedures.