Item 8

Carmel Education Trust

E-Safety Policy

Document Management:	
Date Policy Approved:	8 January 2015
Date Amended:	January 2018
Next Review Date:	January 2021
Version:	2
Approving Body	Student Enrichment Committee

Contents

Background

Scope of the Policy

Roles and Responsibilities

- Directors
- Governors
- Heads[1] and Senior Leaders
- E-Safety Co-ordinators
- IT Manager / Technical Staff
- Teaching and Support Staff
- Designated Persons for Child Protection
- E-Safety Committees
- Students[2]
- Parents / Carers
- Community Users

Policy Statements

- Education – Students
- Education – Parents[3]
- Education – Extended Schools
- Education and training – Staff
- Training – Governors & Directors
- Technical – infrastructure / equipment, filtering and monitoring
- Curriculum
- Use of digital and video images
- Data protection
- Communications
- Unsuitable / inappropriate activities
- Responding to incidents of misuse

[1] In this policy the word 'head' refers to Principals, Head Teachers and Heads of School

[2] In this policy the word 'student' refers to any child or young person studying at one of the trust's academies

[3] In this policy the word 'parent' also refers to carers.

Background

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

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and students / pupils 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 schools are bound. An e-safety policy helps 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 Directors and chief executive, heads and governors to the senior leaders and teachers, support staff, parents, members of the community and the students / pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student achievement.

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

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to, loss of or sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing or distribution of personal images without an individual's consent or knowledge
- Inappropriate communication or contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video or 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 real world and it is essential that this e-safety policy is used in conjunction with other trust and school policies (e.g. behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' / pupils' 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.

The Trust and academies 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.

Related Guidance

The Department for Education (DfE) has published an updated version of its statutory safeguarding guidance, Keeping Children Safe in Education, which is in force from 5 September 2016. The guidance includes information about safeguarding children online.

The guidance requires that children should be safeguarded from potentially harmful and inappropriate online material, and that schools:

‘should ensure appropriate filters and appropriate monitoring systems are in place’.

The guidance requires that as part of their duties under the Prevent Strategy, that schools:

"should ensure that children are safe from terrorist and extremist material when accessing the internet in schools".

The guidance notes, however, that schools must be careful that to ensure that

"over blocking" does not lead to "unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding".

The guidance advices that when considering online safety measures, schools should take into account:

- The age range of pupils
- The number of pupils
- How often they access the school's IT systems
- The proportionality of costs versus the risks

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers, ‘to such extent as is reasonable’, to regulate the behaviour of students or pupils when they are off the school site and empowers members of staff to impose disciplinary penalties within schools for any such inappropriate behaviour. This may be pertinent to incidents of cyber-bullying, or other e-safety incidents involving pupils or students covered by this policy, which may take place out of school, but is linked to membership of the school. In accordance with DfE Guidance (Cyberbullying Advice for Headteachers and School Staff) our schools will handle cyberbullying as a "community issue" on a whole-school level, and ensure that they provide an environment where both staff and pupils are free from harassment and bullying.

Our schools will:

- Support parents in helping their children engage safely and responsibly with social media

- Encourage all members of the community, including parents, to use social media responsibly
- Develop whole-school policies and practices for combating bullying, including cyberbullying and sexting
- Ensure that sanctions are appropriate and consistent
- Ensure routes for reporting incidents are clear

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where appropriate, inform parents of incidents of inappropriate e-safety behaviour that come to the school's attention, but which have taken place out of school. If there are safeguarding aspects to any such incidents, then the school's safeguarding procedures will take precedence.

These headteacher powers are limited to non-criminal bad behaviour, and since cyber bullying may be criminal under the Malicious Communications Act, schools cannot necessarily investigate such incidents happening outside school. E-safety incidents involving the accessing of unsuitable websites outside school would not come under these provisions, but may be safeguarding incidents which could potentially be dealt with under school's safeguarding arrangements.

Roles and Responsibilities

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

Directors:

Directors are responsible for the approval of the E-Safety Policy and for monitoring its effectiveness. This will be carried out by the Student Enrichment Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Board of Directors has taken on the role of Safeguarding Director. The role of the Safeguarding Director will include:

- meetings with the academies' Safeguarding Governors
- monitoring and review of the annual safeguarding audit
- reporting to the Student Enrichment Committee/ Board of Directors annually

Governors:

Governors are responsible for the implementation of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Local Management Board receiving regular information about e-safety incidents through their Headteacher report. A member of each Local Management Board has taken on the role of Safeguarding Governor. The Safeguarding Governor will:

- have regular meetings with the academy's E-Safety Co-ordinator
- review e safety as part of the annual safeguarding audit
- reporting to relevant Governors meeting(s)

Heads and Senior Leaders:

- The Head of each academy is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to an E-Safety Co-ordinator.
- The Heads are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- The Heads will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-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 Teams will each receive regular monitoring reports from the E-Safety Co-ordinator.
- The Head of each academy and another member of the Senior Leadership will follow Trust safeguarding procedures in the event of a serious e-safety allegation being made against a member of staff.

E-Safety Coordinator:

Each academy will have a named member of staff with a day to day responsibility for e-safety (this will be the Designated Safeguarding Lead). The E-Safety Coordinator:

- leads the e-safety committee where the academy head has determined that such a committee should exist
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies and procedures
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the Trust
- liaises with Trust ICT technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments,
- meets regularly with Safeguarding Governor to discuss current issues and review any reported incidents
- attends relevant meetings of Directors and or Governors
- reports regularly to Senior Leadership Team

IT Manager:

The IT Manager is responsible for ensuring that:

- the Trust's ICT infrastructure is secure and is not open to misuse or malicious attack
- the Trust meets the e-safety technical requirements expected of schools and academies, the Trust's Acceptable Usage Policy and the Trust's E-Safety Policy and guidance
- users may only access the school's networks through Trust provided credentials and will adhere to the Acceptable Use Policy
- the Trust's filtering protocols are applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person

- he/she keeps 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
- the use of the Trust's ICT system is regularly monitored in order that any misuse or attempted misuse can be reported to the E-Safety Co-ordinator and Head for investigation and action
- monitoring systems are implemented and regularly

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 Trust e-safety policy and practices
- they have read, understood and signed the staff Acceptable Use Policy
- they report any suspected misuse or problem to the E-Safety Co-ordinator for action
- digital communications with students should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other school activities
- students understand and follow the school 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 school 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 school 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 & Deputy(s)

The Designated Safeguarding Lead and their Deputy (s) will be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers / peers
- potential or actual incidents of grooming
- cyber-bullying, youth produced sexual imagery (often referred to as sexting)
  (NB. it is important to emphasise that these are child protection issues, not technical issues; the technology simply provides additional means for child protection issues to develop)

E-Safety Committee

Members of the E-safety committee (where deemed necessary by the Head) will assist the E-Safety Coordinator or any other relevant person with:

- the implementation and monitoring of the Trust e-safety policy

Students / pupils

- are responsible for using the school IT systems in accordance with the Student Acceptable Use Policy, which they will be expected to sign before being given access to school systems. (NB. at KS1 it is expected that parents will sign on behalf of the pupils)
- should develop 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 school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school 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 school and realise that the school's E-Safety Policy can cover their actions out of school.

Parents / Carers

Parents / Carers can play a crucial role in ensuring that their children understand the need to use the internet or 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 school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature. Parents and carers will be responsible for:

- accepting (by signature) the Student Acceptable Use Policy
- accessing the school website, or other ICT systems in accordance with the relevant Acceptable Use Policy.

The Trust will provide a link to Parent Info http://parentinfo.org/ which provides a free online news feed and access to a collection of articles, tips, expert advice and resources designed to help parents keep up with what their children are doing on-line.

Community Users

Community Users who access school ICT systems as part of the community provision will be expected to sign an Acceptable Use Policy before being provided with access to school systems.

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 e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience. E-Safety education will be provided in the following ways:

- A planned e-safety programme including on-line risks should be provided as part of ICT or other lessons and should be regularly revisited. This will cover both the use of ICT and new technologies in school and outside school and the following risks:
    - Content - being exposed to illegal, inappropriate or harmful material

- Contact - being subjected to harmful online interaction with other users
- Conduct - personal online behaviour that increases the likelihood of, or causes, harm

- Key e-safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities
- Students should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information
- Students / pupils should be helped to understand the need for the student / pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems / internet will be posted in all rooms and displayed on log-on screens
- Staff should act as good role models in their use of ICT, the internet and mobile devices

Education – parents

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 school will therefore seek to provide information and awareness to parents and carers through a variety of means.

Education - Extended Schools

The academies may offer family learning courses in ICT, media literacy and e-safety so that parents and children can together gain a better understanding of these issues. Messages to the public around e safety should also be targeted towards grandparents and other relatives as well as parents. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

Education & Training – Staff

It is essential that all staff receive e-safety training as part of the overarching approach to safeguarding and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the performance management process.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies
- The E-Safety Coordinator (or other nominated person) will receive regular updates through attendance at training sessions and by reviewing appropriate guidance documents
- This E-Safety policy and its updates will be presented to and discussed by staff in staff, department or team meetings or INSET days.

- The E-Safety Coordinator (or other nominated person) will provide advice or training as required to individuals as required

Training – Directors and Governors

Governors should take part in e-safety training sessions, with particular importance for those who are members of any group involved in ICT, e-safety, health and safety or child protection. This may be offered in a number of ways:

- Attendance at training provided by a relevant organisation
- On-line training, e.g. provided by GEL
- Participation in school training / information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

The IT Manager will be responsible for ensuring that the Trust 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 e-safety responsibilities:

- There will be regular reviews and audits of the Trust's safety and security of school ICT systems
- Servers, wireless systems and cabling wherever possible will be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems**.** *Details of the* access rights available to groups of users will be recorded by the IT Manager and will available for review by the Safeguarding Director, Chief Executive Officer and Heads.
- All users will be provided with a username and password.
- The "administrator" passwords for the school ICT system, used by the IT Manager (or other person) must also be available to the Head or other nominated senior leader and kept in a secure place
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The Trust maintains and supports a managed filtering service sufficient to ensure that the Trust is able to meet its duty to ensure the safety of all users
- In the event of the IT Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Chief Executive Officer
- Any filtering issues should be reported immediately to the Chief Executive Officer
- Requests from staff for sites to be removed from the filtered list will be considered by the IT Manager. If the request is agreed, this action will be recorded and may be reviewed by the E-Safety Committee
- School IT technical staff regularly monitor and record the activity of users on the school IT systems and users are made aware of this in the Acceptable Use Policy
- Remote management tools are used by staff to control workstations and view users' activity
- An appropriate system is in place for users to report any actual / potential e-safety incident to the IT Manager (or other relevant person).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- The school infrastructure and individual workstations are protected by up to date virus software.

Curriculum

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

- in lessons where internet use is 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 they visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, homophobia or discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager (or other relevant person) 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 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

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 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.

Please see Trust Photographic policy for details.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998, the General Data Protection Regulations and the Trust's Data Protection & Information Security Policies.

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning.

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – in accordance with the school policy, 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 must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Whole class or group email addresses may be used at KS1, while students in KS2 and above will be provided with individual school email addresses for educational use. (Schools may choose to use group or class email addresses for younger age groups e.g. at KS1)
- 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 school website and only official email addresses should be used to identify members of staff.

The Trust has different expectations of different groups within the school community: staff, students in each of the Key Stages of education and adult members of the sider school community. Please see the relevant Acceptable use Policy.

Responding to incidents of misuse

It is expected that all members of the school 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 deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity e.g.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

The police must be informed and the Chief Executive Officer should be briefed (if not inappropriate).

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that appropriate procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event it is recommended that more than one member of staff is involved in the investigation which should be carried out on a “clean” designated computer.

It is more likely that the school 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 or disciplinary procedures. Please see the Trust’s, and/or the individual academy’s Behaviour Policy, Staff Code of Conduct and Acceptable Use Policy.