# E-Safety Policy

Date written- December 2017
Review Date – December 2018

The e-Safety Policy is part of the Computing and Safeguarding Policies. It also relates to the Academy vision statement and other policies including those for behaviour, anti-bullying, personal, social and health education (PSHE) and for citizenship.

## Teaching and learning

### Why is Internet use important?

The rapid developments in electronic communications are having many effects on society. It is important to state what we are trying to achieve in education through Computing and Internet use. Internet use is part of the statutory curriculum and a necessary tool for learning.

- The Internet is a part of everyday life for education, business and social interaction. The academy has a duty to provide students with quality Internet access as part of their learning.
- Pupils use the Internet widely outside academy and need to learn how to evaluate Internet information and to take care of their own safety and security.
- The purpose of Internet use in academy is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.

### How does Internet use benefit education?

Studies and government projects have identified the educational benefits to be gained through the appropriate use of the Internet including increased pupil attainment. Benefits of using the Internet in education include among others:

- access to world-wide educational resources including museums and art galleries;
- educational and cultural exchanges between pupils world-wide;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across networks of school, support services and professional associations;
- exchange of curriculum and administration data
- access to learning wherever and whenever convenient.

### How can Internet use enhance learning?

Increased computer and iPad numbers and improved Internet access may be provided but its impact on pupils' learning outcomes should also be considered. Developing effective practice in using the Internet for teaching and learning is essential. Pupils need to learn digital literacy skills and to refine their own publishing and communications with others via the Internet. Respect for copyright and intellectual rights, and the correct use of published material should be taught. The academy's Internet access is designed to enhance and extend education. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. The academy will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law. Staff should guide pupils to on-line activities that will support the learning outcomes planned for the pupils' age and maturity. Pupils will be educated in the effective use of Internet research, including the skills of knowledge location, retrieval and evaluation.

**How will pupils learn how to evaluate Internet content?**
Information received via the Internet, email or text message requires information handling and digital literacy skills. It may be difficult to determine origin, intent and accuracy, as the contextual clues may be missing or difficult to read. Researching potentially emotive themes provide an opportunity for pupils to develop skills in evaluating Internet content. Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. This includes how to narrow searches so that they receive more of the information they require.

**Managing Information Systems**

**How will information systems security be maintained?**
It is important to review the security of the whole system from user to Internet. This is a major responsibility that includes not only the delivery of essential learning services but also the personal safety of staff and pupils.

**Local Area Network (LAN) security issues include:**
Workstations should be secured against user mistakes and deliberate actions. Servers are located securely and physical access restricted. The server operating system will be secured and kept up to date. Virus protection for the whole network must be installed and current. Access by wireless devices must be pro-actively managed. Users must adhere to the acceptable use policy.

- The security of the academy information systems and users will be reviewed regularly.
- Virus protection will be updated regularly.
- Personal data sent over the Internet or taken off site will be encrypted.
- Unapproved software will not be allowed in pupils' work areas or attached to email.
- Files held on the school's network will be regularly checked.

**How will email be managed?**
Email is an essential means of communication for both staff and pupils. Directed email use can bring significant educational benefits and interesting projects between schools. The implications of email use for the schools and pupils need to be thought through and appropriate safety measures put in place. Un-regulated email can provide routes to pupils that bypass the traditional academy boundaries. A central question is the degree of responsibility that can be delegated to individual pupils as once email is available it is difficult to control. Restriction of incoming and outgoing email to approved addresses and filtering for unsuitable content is possible. In the school context (as in the business world), email should not be considered private and most academy and many firms reserve the right to monitor email. There is a balance to be achieved between necessary monitoring to maintain the safety of pupils and the preservation of human rights, both of which are covered by recent legislation. Email accounts should not be provided which can be used to identify both a student's full name and their academy. Spam, phishing and virus attachments can make email dangerous.

- Pupils may only use approved email accounts.
- Pupils must immediately tell a teacher if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication
- Access in the academy to external personal email accounts is not allowed.
- Email sent to external organizations should be written carefully and authorized before sending, in the same way as a letter written on academy headed paper.
- The forwarding of chain messages is not permitted.
- Staff should not use personal email accounts during academy hours or for professional purposes.

**How will published content be managed?**
The academy has created an excellent website that inspires pupils to publish work of a high standard. Sensitive information such as personal details will not be published.

- The contact details on the website will be the academy address, email and telephone number.
- Staff or pupils' personal information must not be published.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with the academy's guidelines for publications including respect for intellectual property rights and copyright.
- Work/photos will only be published in line with parental permission.

**Can pupil's images or work be published?**
Still and moving images and sounds add interest to a publication. Nevertheless, the security of staff and pupils is paramount. The publishing of pupils' full names with their images is not acceptable. Published images could be re-used, particularly if large images of individual pupils are shown. Strategies include using relatively small images of groups of pupils and possibly even using images that do not show faces at all. Pupils in photographs should, of course, be appropriately clothed. Images of a pupil should not be published without the parent's or carer's permission. Pupils also need to be taught the reasons for caution in publishing personal information and images online.

- Images that include pupils will be selected carefully and will not provide material that could be reused.
- Pupils' full names will not be used anywhere on the website/media, particularly in association with photographs.
- Permission from parents or carers will be checked before images of pupils are electronically published.
- Children will be taught to ask if they would like to take a photo/video of someone.
- Photos of other people will not be sent to other children without their permission, particularly via ipads.
- Photographs taken by staff will be stored appropriately.

**How will social networking, social media and personal publishing be managed?**
Online spaces and social networks allow individuals to publish unmediated content. Users can be invited to view personal spaces and leave comments, over which there may be limited control. For responsible adults, social networking sites provide easy to use, free facilities; although often advertising intrudes and may be dubious in content. Pupils should be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published. All staff should be made aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. They should be made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status. Examples include: blogs, wikis, social networking, forums, bulletin boards, multi-player online gaming, chatrooms, instant messenger and many others.

- The academy network will not allow access to social media and social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Pupils should be advised not to place personal photos on any social network space. Advice should be given regarding background detail in a photograph which could identify the student or his/her location.
- Staff will be advised not to run social network spaces for pupil use on a personal basis.

- If personal publishing is to be used with pupils, then it must use age appropriate sites suitable for educational purposes. Personal information must not be published, and the site should be moderated by academy staff.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others by making profiles private.
- Pupils are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or insulting. Staff, along with external professionals, will teach children how to use sites securely and safely.

**How will filtering be managed?**

Levels of Internet access and supervision will vary according to the pupil's age and experience. Access profiles must be appropriate for all members of the academy community. Teachers might need to research areas including drugs, medical conditions, bullying, racism or harassment. In such cases, legitimate use should be recognised and restrictions removed temporarily. Systems to adapt the access profile to the pupil's age and maturity are available. Access controls fall into several overlapping types (commonly described as filtering):

- Blocking strategies prevent access to a list of unsuitable sites. Maintenance of the blocking list is a major task as new sites appear every day.
- A walled-garden or "allow-list" restricts access to a list of approved sites.
- Dynamic filtering examines emails for unsuitable words. Access monitoring records the Internet sites visited by individual users. Attempted access to a site forbidden by the policy will result in a report.
- If staff or pupils discover unsuitable sites, the URL must be reported to the e-Safety Coordinator/oneIT. The academy's broadband access will include filtering appropriate to the age and maturity of pupils.
- OneIT will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the academy believes is illegal must be reported to appropriate agencies such as CEOP or ONE IT.

**How can emerging technologies be managed?**

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, Internet access, collaboration and multimedia tools. Virtual online classrooms and communities widen the geographical boundaries of learning. The safety and effectiveness of virtual communities depends on users being trusted and identifiable. This may not be easy, as authentication beyond the academy may be difficult as demonstrated by social networking sites such as Bebo, Instagram and Facebook. The registering of individuals to establish and maintain validated electronic identities is essential for safe communication, but is often not possible. Video conferencing introduces new dimensions; webcams are increasingly inexpensive and, with faster Internet access, enable video to be exchanged across the Internet. The availability of live video can sometimes increase safety - you can see who you are talking to. There are dangers for staff however if personal phones are used to contact pupils and therefore an academy owned phone should be issued.

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in academy is allowed.
- Staff will be issued with an academy phone where contact with pupils/parents/carers is required.
- Mobile phones will not be used during lessons or formal academy time, unless on a school visit

where it is an essential call. Mobile phones can only be used in the staffroom, and not in classrooms or other academy areas.

**How should personal data be protected?**

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused. The Data Protection Act 1998 ("the Act") gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information. Under the Act every organization that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Act sets standards which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights lets individuals find out what information is held about them. The eight principles are that personal data must be:

- Processed fairly and lawfully
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Held no longer than is necessary
- Processed in line with individual's rights
- Kept secure
- Transferred only to other countries with suitable security measures.

Schools already have information about their obligations under the Act, and this section is a reminder that all data from which people can be identified is protected.

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

**Policy Decisions**

**How will Internet access be authorized?**

The academy should allocate Internet access for staff, pupils, visitors and the community based on educational need. It should be clear who has Internet access and who has not. In a primary school, where pupil usage should be fully supervised, most pupils will be granted Internet access; it may be easier to manage lists of those who are denied access. Parental permission will be required for Internet access in all cases — a task that may be best organized annually when pupils' home details are checked, and as new pupils join.

- All staff must read and sign the 'Staff Acceptable Use Policy' before using any academy ICT resource.
- Trustees will review the policy in line with timescales.
- Parents will be asked to sign and return a consent form for pupil access.
- Parents will be informed that pupils will be provided with supervised Internet access.

**How will risks be assessed?**

As the quantity and breadth of information available through the Internet continues to grow it is not possible to guard against every undesirable situation. The academy will need to address the issue that it is not possible to completely remove the risk that pupils might access unsuitable materials via the academy system.

- The academy will take all reasonable precautions to ensure that users access only appropriate material. Neither the academy nor TVED can accept liability for the material accessed, or any consequences resulting from Internet use.
- The academy should audit ICT use to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

**How will e–Safety complaints be handled?**

Parents, teachers and pupils should know how to use the School's complaints procedure. The facts of the case will need to be established, for instance whether the Internet use was within or outside academy. A minor transgression of the rules may be dealt with by a member of staff. Other situations could potentially be serious, and a range of sanctions will be required, linked to the school's disciplinary policy. Potential child protection or illegal issues must be referred to the academy Designated Child Protection Coordinator or e–Safety Coordinator. Advice on dealing with illegal use could, when deemed necessary, be discussed with the Police Safer Schools Partnership Coordinator responsible for the academy or the Children's Safeguard Unit.

- Complaints of Internet misuse will be dealt with under the Academy's Complaints Procedure.
- Any complaint about staff misuse must be referred to the headteacher.
- All e–Safety complaints and incidents will be recorded by the academy, including any actions taken.
- Pupils and parents will be informed of the complaints procedure. Parents and pupils will work in partnership with staff to resolve issues.
- Discussions will be held with the local Police Safer Academy Partnership Coordinators and/or Children's Safeguards Unit to establish procedures for handling potentially illegal issues.
- Any issues (including sanctions) will be dealt with according to the Academy's disciplinary and child protection procedures.
- Trustees will be informed as necessary.

**How is the Internet used across the community?**

Internet access is available in many situations in the local community. In addition to the home, access may be available at the local library or youth club. Ideally, young people would encounter a consistent policy to Internet use wherever they are. In community Internet access there is a fine balance to be achieved in ensuring open access to information whilst providing adequate protection for children and others who may be offended by inappropriate material.

- The academy will be sensitive to Internet related issues experienced by pupils out of academy, e.g. social networking sites, and offer appropriate advice and support.

**How will Cyberbullying be managed?**

Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" DCSF 2007. Many young people and adults find using the internet and mobile phones a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. When children are the target of bullying via mobiles phones, gaming or the internet, they can often feel very alone, particularly if the adults around them do not understand cyberbullying and its effects. It is essential that young people, academy staff and parents and carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety. DCSF and Childnet have produced

resources and guidance that can be used to give practical advice and guidance on cyberbullying: http://www.digizen.org/cyberbullying

- Cyberbullying (along with all forms of bullying) will not be tolerated in academy. Full details are set out in the school's policy on anti-bullying.
- There will be clear procedures in place to support anyone effected by cyberbullying.
- All incidents of cyberbullying reported to the academy will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of cyberbullying:
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The academy will take steps to identify the bully, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.

Sanctions for those involved in cyberbullying may include:

- The bully will be asked to remove any material deemed to be inappropriate or offensive.
- A service provider may be contacted to remove content.
- Internet access may be suspended at academy for the user for a period of time.
- Parent/carers will be informed.
- The Police will be contacted if a criminal offence is suspected.

**Marvellous Me**

Engaging parents/carers has a proven track record of raising achievement of their children. Marvellous Me, an app, allows staff to communicate in appositive manner on regular intervals with parents/carers.

- Staff will send positive messages.
- Only images of their child will be sent, with prior permission from parents/carers.

**Communication Policy**

**How will the policy be introduced to pupils?**

Many pupils are very familiar with mobile and Internet use and culture and it is wise to involve them in designing the e-Safety Policy, possibly through a student council. As pupils' perceptions of the risks will vary; the e-Safety rules may need to be explained or discussed. The pupil and parent agreement form should be attached to a copy of the Academy e-Safety rules appropriate to the age of the pupil.

Useful e-Safety websites include:

Think U Know: www.thinkuknow.co.uk

Childnet: www.childnet.com

Kidsmart: www.kidsmart.org.uk

- All users will be informed that network and Internet use will be monitored.
- An e-Safety module will be included in the PSHE, Citizenship and/or ICT programmes covering both safe academy and home use.
- Safe and responsible use of the internet and technology will be reinforced across the curriculum.
-

**How will the policy be discussed with staff?**

It is important that all staff feel confident to use new technologies in teaching and the Academy e-Safety Policy will only be effective if all staff subscribe to its values and methods. Staff should be given opportunities to discuss the issues and develop appropriate teaching strategies. It would be unreasonable, for instance, if cover or supply staff were asked to take charge of an Internet activity without preparation. If a member of staff is concerned about any aspect of their ICT use in

academy, they should discuss this with their line manager to avoid any possible misunderstanding. Consideration must be given when staff are provided with devices by the academy which may be accessed outside of the academy network. The Academy must be clear about the safe and appropriate use of academy provided equipment and rules about use of the equipment by third parties. Staff must be made aware of their responsibility to maintain confidentiality of academy information. Induction of new staff should include a discussion of the academy e–Safety Policy.

- The e–Safety Policy will be formally provided to and discussed with all members of staff.
- To protect all staff, pupils, visitors and community users, the academy will implement Acceptable Use Policies.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff training in safe and responsible Internet use both professionally and personally will be provided.

**How will parents' support be enlisted?**

Unless parents are aware of the dangers, pupils may have unrestricted and unsupervised access to the Internet in the home. The academy may be able to help parents plan appropriate supervised use of the Internet at home and educate them on the risks. Parents should also be advised to check if their child's use elsewhere in the community is covered by an appropriate use policy.

- Parents' attention will be drawn to the Academy e–Safety Policy on the academy website.
- A partnership approach with parents will be encouraged. This will include parent sessions with demonstrations and suggestions for safe home Internet use or highlighting e–Safety at other attended events e.g. parent evenings, sports days.
- Parents will be requested to sign an e–Safety/internet agreement as part of the Home Academy Agreement.
- Information and guidance for parents on e–Safety will be made available to parents in a variety of formats.

## Legal Framework

### Notes on the legal framework

This section is designed to inform users of potential legal issues relevant to the use of electronic communications. It is not professional advice. Many young people and indeed some staff use the Internet regularly without being aware that some of the activities they take part in are potentially illegal. The law is developing rapidly and changes occur frequently.

### Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

### Criminal Justice Act 2003

Section 146 of the Criminal Justice Act 2003 came into effect in April 2005, empowering courts to impose tougher sentences for offences motivated or aggravated by the victim's sexual orientation in England and Wales.

### Sexual Offences Act 2003

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). This can include images taken by and distributed by the child themselves (often referred to as "Sexting"). A person convicted of such an offence may face up to 10 years in prison. The offence of grooming is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification.

N.B. Academy should already have a copy of "Children & Families: Safer from Sexual Crime" document as part of their child protection packs. More information about the 2003 Act can be found at www.teachernet.gov.uk

### Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

### Data Protection Act 1998

The Act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

**The Computer Misuse Act 1990 (sections 1 — 3)**
Regardless of an individual's motivation, the Act makes it a criminal offence to:

- gain access to computer files or software without permission (for example using someone else's password to access files);
- gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or
- Impair the operation of a computer or program (for example caused by viruses or denial of service attacks). UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

**Malicious Communications Act 1988 (section 1)**
This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

**Copyright, Design and Patents Act 1988**
Copyright is the right to prevent others from copying or using his or her "work" without permission. The material to which copyright may attach (known in the business as "work") must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a license or in ways prohibited by the terms of the software licence.

**Public Order Act 1986 (sections 17 — 29)**
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

**Obscene Publications Act 1959 and 1964**
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

**Protection from Harassment Act 1997**
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

**Regulation of Investigatory Powers Act 2000**
The Regulation of Investigatory Powers Act 2000 (RIP) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications

are relevant to academy activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

**Criminal Justice and Immigration Act 2008**
Section 63 offence to possess "extreme pornographic image" 63 (6) must be "grossly offensive, disgusting or otherwise obscene" 63 (7) this includes images of "threats to a person life or injury to anus, breasts or genitals, sexual acts with a corpse or animal whether alive or dead" must also be "explicit and realistic" Penalties can be up to 3 years imprisonment.

Education and Inspections Act 2006
Education and Inspections Act 2006 outlines legal powers for academy which relate to Cyberbullying/Bullying:

Headteachers have the power "to such an extent as is reasonable" to regulate the conduct of pupils off site.

Academy staff are able to confiscate items such as mobile phones etc when they are being used to cause a disturbance in class or otherwise contravene the academy behaviour/antibullying policy.