CORE
EDUCATION
TRUST

E-Safety Policy

September 2020

DELIVERING A
CORE EDUCATION

Contents

1. Rationale
2. Aims and Objectives
3. Scope of the E-Safety Policy
4. Roles and Responsibilities
5. Education and Training
6. The Acceptable Use of ICT, Including Social Media
7. Monitoring and Responding to Incidents of E-Safety
8. Extremism and Radicalisation

Appendix 1

Appendix 2

Appendix 3

1. Rationale

1.1 With the increasing availability of devices which give unrestricted access to the internet for children, CORE Education Trust considers online safety to be extremely important. We endeavor to ensure that every pupil in CORE's care is safe; and the same principles apply to the digital world as apply to the real world. This policy applies to all CORE staff, volunteers, visitors, parents/carer and pupils.

1.2 IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and more subtle risks to young people. CORE Education Trust has a responsibility to provide a safe environment in which children can learn. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of identity theft, cyber-bullying, radicalisation, harassment, grooming, stalking and abuse.

2. Aims and objectives

2.1 The aim of this policy is to establish the ground rules we have in school for using ICT equipment and the Internet. New technologies have become integral to the lives of children and young people in today's society, both within educational establishments and in their lives outside school.

2.2 The Internet and other digital/information technologies are powerful tools which open up new opportunities for everyone but there are risks attached to them. Some of the dangers our pupils 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/distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication/contact with others, including strangers.
- Cyber-bullying.
- Extremism and radicalization.
- Child Sexual Exploitation.
- 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.

2.3 Many of these risks reflect situations in the off-line world and it is essential that this e- safety policy is read and used in conjunction with other school policies; specifically, Anti- Bullying, Behaviour and Safeguarding and Child Protection.

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

2.5 The school provides the necessary safeguards to help ensure that we have done everything that could reasonably be expected to manage and reduce these risks. The e- safety policy explains how the school intends to do this, whilst also addressing wider educational issues in order to help young people (and their parents/carers and staff) to be responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use.

3. Scope of the E-safety policy

3.1 The School's E-safety policy is in line with the following national frameworks most recent versions:

- Keeping Children Safe in Education.
- Ofsted Common Inspection Framework.
- The Prevent Duty.
- Working together to safeguard children.
- The Prevent Strategy (June 2011) and Channel guidance.

3.2 This policy has links to the following policies:

- Safeguarding and Child Protection Policy.
- Behaviour for Learning.
- Anti-bullying.
- Data Protection.
- Professional Code of Conduct.
- Acceptable Usage Policy.

3.3 This policy applies to all members of the school community (including staff, pupils, governors, volunteers, parents/carers and visitors) who have access to and are users of school IT systems, both in and out of school. This policy, supported by the Acceptable Use Policy for all staff and pupils, is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements.

3.4 The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

3.5 This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

3.6 The school will deal with such incidents within this policy and in associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

4. Roles & Responsibilities

This section outlines the roles and responsibilities for e-safety of individuals and groups within the school.

4.1 Governance

The Board of Directors are responsible for the approval of the trust e-safety policy. The Local Governing Body of each school is responsible for reviewing the effectiveness of the policy. A member of the Governing Body is responsible for Safeguarding/Child Protection and E-Safety will be a part of this.

4.2 Headteacher

The Headteacher is responsible for ensuring the safety (including e-safety) of all members of the school community, although the day to day responsibility for e-safety is delegated to the Designated E-Safety Lead, ICT Network Manager, and the Head of ICT, or equivalent roles.

4.3 Designated Senior Leader

The Designated Senior Leader takes day to day responsibility for e-safety issues and has a leading role in:

- Liaising with staff, the LA, ICT Network Manager, Safeguarding Governor and SLT on all issues related to e-safety, including Child Sexual Exploitation and extremism and radicalization.
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Adequate training is provided for staff in e-safety, including Child Sexual Exploitation and extremism and radicalization.
- Effective recording and monitoring systems are set up and outcomes are rigorously analysed.
- Maintaining a system to provide pupils with an avenue to report concerns.
- Co-ordinating and reviewing an e-safety education programme in school.
- That relevant procedures in the event of an e-safety allegation are known and understood.
- Establishing and reviewing the school e-safety policies and documents.
- The school's Designated Child Protection Officers are trained in e-safety issues and be aware of the potential for serious child protection issues to arise using IT.

4.4 School ICT Network Manager

The Network Manager (or equivalent role or where a managed service a designated member of staff within the management service team) is responsible for ensuring that:

- The school's ICT infrastructure is secure and meets e-safety technical requirements.
- The school's password policy is adhered to.
- The school's filtering and monitoring system is applied and updated on a regular basis.
- The Network Manager keeps up to date with e-safety technical information.
- The use of the school's ICT infrastructure (network, remote access, e-mail, VLE etc.) is regularly monitored in order that any misuse or attempted misuse can be reported to the Designated E-Safety Lead for investigation/action/sanction.

4.5 Teaching & Support Staff

All teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current school e- safety policy and practices.
- They have read, understood, and signed the school Staff Social Media and Social Networking Policy.

- E-safety issues are embedded in all aspects of the curriculum and other school activities.
- Pupils understand and follow the school's e-safety policy and follow the guidelines on acceptable internet use in their planners.
- They monitor ICT activity in lessons, extracurricular and extended school activities.
- In lessons where Internet use is pre-planned, pupils 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.

4.6 Pupils

- Are responsible for using the school ICT systems in accordance with the guidance contained in their planners.
- All pupils are asked to sign in their planner an agreement pertaining to social media usage.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know that avenues are available to allow them to do this.
- 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 also cover their actions out of school.

4.7 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 school will therefore take opportunities to help parents understand these issues.
Parents and carers will be responsible for:

- Endorsing via signature the guidance pertaining to social media and social networking.
- Attending advice sessions that CORE Education Trust's schools provide for parents.

5. Education and Training

5.1 E-safety education will be provided in the following ways:

- E-Safety advice is provided as part of the class teacher/form tutor and assembly programme and is regularly revisited in Information Technology and other lessons across the curriculum.
- Pupils are taught in lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of the information.
- Pupils are encouraged to adopt safe and responsible use of ICT, the Internet, and mobile devices both within and outside of school during designated lessons and curriculum areas.
- Pupils are taught about e-safety in the context of extremism and radicalisation and Child Sexual Exploitation.
- Rules for the use of ICT systems and the Internet are regularly available to pupils (E.g.: opening screen message; pupil planner as appropriate).
- Staff act as good role models in their use of ICT, the Internet and mobile devices.

5.2 Staff Training

- The school will ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- E-Safety training will be provided to staff as part of their wider safeguarding responsibilities and will include a focus on Child Sexual Exploitation and extremism and radicalisation.
- All staff will participate in the Workshop Raising Awareness of Prevent (WRAP).
- All new staff receive the school E-Safety, Safeguarding and Child Protection Policies and the latest version of Keeping Children Safe in Education and the school ensures that these documents are understood.
- The designated Senior lead will receive regular updates through the Local Authority and/or other information/training sessions and by reviewing guidance documents released.

6. The Acceptable Use of ICT, Including Social Media

6.1 Email

- Digital communications with pupils (e.g. e-mail) should be on a professional level and only carried out using official school systems.
- Under no circumstances should staff contact pupils, parents/carers or conduct any school business using personal e-mail addresses.
- School e-mail is not to be used for personal use.

6.2 Mobile Phones

- School mobile phones only should be used to contact parents/carers/pupils when on school business with pupils off site. Staff should not use personal mobile devices.
- Staff should not be using personal mobile phones in school during working hours when in contact with children.
- Pupils should adhere to the rules and guidelines set out in the Behaviour Policy regarding mobile phone use in school.

6.3 Social Networking Sites

Young people will not be allowed on social networking sites at school; at home it is the parental responsibility, but parents should be aware that it is illegal for children under the age of 13 to be on certain social networking sites.

- Staff should not access social networking sites on school equipment in school or at home. Staff should access sites using personal equipment.
- Staff users should not reveal names of staff, pupils, parents/carers or any other member of the school community on any social networking site or blog.
- Pupils/Parents/carers should be aware the school will investigate misuse of social networking if it impacts on the well-being of other pupils or stakeholders.
- If inappropriate comments are placed on social networking sites about the school or school staff then advice would be sought from the relevant agencies, including the police if necessary.

- Pupils will be taught about e-safety on social networking sites as we accept some may use it outside of school. This will take place in designated lessons and/or themed days, during form time and within assemblies.

6.4 Digital Images

- The school record of parents who do not wish photos to be taken of their child is available from the relevant administrator in each school.
- Under no circumstances should images be taken using privately owned equipment without the express permission of the Headteacher.
- Where permission is granted the images should be transferred to school storage systems and deleted from privately owned equipment at the earliest opportunity.

Although many of the above points are preventative and safeguarding measures, it should be noted that the school will endeavour whenever possible to use the internet in positive ways to publicise, inform and communicate information. The school has an active website and twitter account which is used to inform, publicise school events and celebrate and share the achievement of pupils.

6.5 Websites

- In lessons where Internet use is pre-planned, pupils 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.
- Staff will preview any recommended sites before use. Certain websites are automatically blocked by the school's filtering system.
- "Open" searches (e.g. "find images/ information on...") are discouraged when working with younger pupils who may misinterpret information.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by staff.
- All users must observe copyright of materials published on the Internet.
- Teachers will judge which pupils are allowed access to the internet with minimal supervision. Minimal supervision means regular checking of the pupils on the internet by the member of staff setting the task. All staff are aware that if they pass pupils working on the internet that they have a role in checking what is being viewed. Pupils are also aware that all internet use at school is tracked and logged.
- The school only allows the Headteacher and the ICT Network Manager to access internet logs.
- Pupils should immediately report, to the Designated E-Safety Lead, Head of ICT or another member of staff the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Pupils must report any accidental access to materials of a violent, disturbing, or sexual nature directly to the Designated E-Safety Lead, Head of ICT or another member of staff. Deliberate access to any inappropriate materials by a pupil will lead to the incident being dealt with under the school's Behaviour for Learning Policy. Pupils should be aware that all internet usage via the school's systems and its Wi-Fi network is monitored.

6.6 Passwords

- Staff passwords or encryption keys should not be recorded on paper or in an unprotected file and should be changed at least every 3 months. Users should not use the same password on multiple systems or attempt to "synchronise" passwords across systems.
- Pupils should not let staff know the passwords they use out of school.
- Pupils must inform staff immediately if passwords are traced or forgotten so they can be reset.

6.7 Use of Own Equipment

- Privately owned ICT equipment should never be connected to the school's network without the specific permission of the Headteacher and/or the ICT Network Manager.
- Pupils should not bring in their own equipment unless asked to do so by a member of staff.

6.8 Use of School Equipment

- No personally owned applications or software packages should be installed on to school ICT equipment.
- Personal or sensitive data (belonging to staff) should not be stored on the local drives of desktop or laptop PCs.
- All staff should ensure any screens are locked (by pressing Ctrl, Alt, Del simultaneously) before moving away from a computer during the normal working day to protect any personal, sensitive, confidential or classified data and to prevent unauthorised access.

6.9 Data Storage

- Staff are expected to save all data relating to their work to their Laptop if they have been assigned one, or to the school's VLE.
- The school discourages the use of removable media however if they are used, we expect the Encryption of all removable media (USB pen drives, CDs, portable drives) taken outside school or sent by post or courier.
- Staff laptops should be encrypted if any data or passwords are stored on them.
- IEPs, assessment records, pupil medical information and any other data related to pupils or staff should not be stored on personal memory sticks but stored on an encrypted USB memory stick provided by school or on the relevant secure platform in the staff area.
- Only take offsite information you are authorised to and only when it is necessary and required to fulfil your role. If you are unsure speak to a member of the Senior Leadership Team.

7. Monitoring and Responding to Incidents of E-Safety

7.1 All use of the school's Internet access is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up by either Middle leaders, Designated E-Safety Lead, or another member of SLT depending on the severity of the incident.

The ICT Network Manager will report any breaches, suspected or actual, of the school filtering systems to Designated E-Safety Lead and the Headteacher. Any member of staff employed by the school who comes across an e-safety issue does not investigate any further but immediately reports it to the Designated E-Safety Lead and impounds the equipment. (If the concern involves the Designated E-Safety Lead then the member of staff should report the issue to the Headteacher).

7.2 Any e-safety incidents must immediately be reported to the Headteacher (if a member of staff) or Designated E-Safety Lead (if a pupil) who will investigate further following e-safety and safeguarding policies and guidance.

It is hoped 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 or irresponsible, or very rarely, through deliberate 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 or other criminal conduct, activity or materials the Police will be contacted in the case of a pupil while the LADO will be contacted in the case of a member of staff to discuss a suitable course of action. If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. 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. The Headteacher will commission and ensure appropriate guidance is provided to staff carrying out such investigations.
It is intended that incidents of misuse will be dealt with through normal behaviour/ disciplinary procedures.

8. Extremism and Radicalisation

8.1 The statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. Schools should ensure that suitable filtering is in place and pupils are safe from radicalisation whilst online.

More generally, schools have an important role to play in equipping children and young people to stay safe online, both in school and outside. Internet safety will be integral to a school's ICT curriculum and can also be embedded in Citizenship. PSHEe and SRE, alongside other areas of the curriculum as appropriate.

As with other online risks of harm, every teacher needs to be aware of the risks posed by the online activity of extremist and terrorist groups and will receive annual training through in-school Safeguarding Training and the Workshop Raising Awareness of Prevent.

Appendix 1

Staff (and Volunteer) Acceptable Use Policy Agreement
School Policy

New technologies have become integral to the lives of children and young people in today' s society, both within school and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open new opportunities for everyone. These technologies can stimulate discussion, promote creativity, and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access always.

This Acceptable Use Policy is intended to ensure:

- That staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal, and recreational use.
- That school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal Safety:

- I understand that the school will monitor my use of the ICT systems, email, and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, VLE etc.) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else nor will I try to use any other person's username and password.
- I will immediately report any illegal inappropriate or harmful material or incident that I become aware of to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.

- I will communicate with others in a professional manner; I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the digital/video. I will not use my personal equipment to record these images unless I have permission to do so. Where these images are published (e.g. on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured. Where personal equipment is used with permission, any images recorded should be deleted from that equipment as soon as possible once the images have been transferred to school systems.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents/carers using official school systems. Any such communication will be professional in tome and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held/external devices (PDAs/laptops/mobile phones/USB devices, etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems during my working hours.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will try not to upload, download or access any materials with are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will try not to use any programmes or software that might allow me to bypass the filtering/security systems in place. To prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent others from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others as outlines in the School Personal Data Policy. Where personal data is transferred outside the secure school network, it must be encrypted. I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or the school policy to disclose such information to an appropriate authority. I will immediately report any damage or faults involving equipment or software; however, this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and in the event of illegal activities the involvement of the police.

I have read and understood the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name: _____

Signed: _____

Date: _____

Appendix 2

Exemplar e- safety agreement for parents/carers and staff

Parents

- There are several important steps you can take to ensure your children are safer when using sites such as Facebook, Twitter, Instagram, Bebo, Snapchat, WhatsApp or KiK.
- Become familiar with the sites yourself.
- Encourage your children to keep their profiles private.
- Be careful about what information your children are sharing on the site. Do you know all your child's online friends?
- Encourage children to think about who they want to add as a friend.
- Make sure your children know where to go for help if they feel uncomfortable.
- If you do not want your children to access these services use parental control devices to block access to the sites.
- Remember that children must be 13 years or older to sign up for Facebook.
- Monitor the amount of time your child is spending on social networking sites.

Pupils

- Be careful with personal information. As soon as information goes online you have lost control over who will see it and how it will be used. Do not post pictures that you would not want everyone to see.
- Do not assume everyone you meet online is who they appear to be. The information provided by users when they register is not checked. Anyone can create a profile pretending to be someone else.
- Do not post information that could be used to find you in the real world.
- Do not reply to messages that harass you or make you feel uncomfortable.
- Always explore the privacy settings of the site to protect your privacy and to protect yourself from strangers.
- Get your friends and family to check your social networking site to check you are doing things safely.
- Keep your passwords to yourself.
- If you are a victim of cyberbullying
  - report the bully to the website.
  - keep evidence of what happened.
  - tell an adult.
- Remember when you post something online you are posting it on the biggest screen in the world which can be seen by billions of people.
- Please sign below to show that you have read the above advice.

Appendix 3

Exemplar advice for pupils and staff

Our advice for parents

- There are several important steps you can take to ensure your children are safer when using sites such as WhatsApp, KiK, Facebook, Myspace or Bebo.
- Become familiar with sites yourself.
- Encourage your children to keep their profiles private.
- Be careful about what information your children are sharing on the sites.
- Do you know all your child's online friends?
- Encourage children to think about who they want to add as a friend.
- Make sure your children know where to go for help if they feel uncomfortable.
- If you do not want your children to access these services use parental control devices to block access to the sites.
- Remember that children must be 13 years or older to sign up for Facebook.
- Monitor the amount of time your child is spending on social networking sites.
- Raise any concerns you have regarding your child immediately to your child's Year Co-ordinator.

Our advice for pupils

- Be careful with personal information. As soon as information goes online you have lost control over who will see it and how it will be used.
- Do not post pictures that you would not want everyone to see.
- Do not assume everyone you meet online is who they appear to be. The information provided by users when they register is not checked. Anyone can create a profile pretending to be someone else.

- Do not post information that could be used to find you in the real world.
- Do not reply to messages that harass you or make you feel uncomfortable.
- Always explore the privacy settings of the site to protect your privacy and to protect yourself from strangers.
- Get your friends and family to check your social networking site to check you are doing things safely.
- Keep your passwords to yourself.
- If you are a victim of cyberbullying
    - report the bully to the website.
    - keep evidence of what happened.
    - tell an adult.
    - the key is to report it.
- Remember when you post something online you are posting it on the biggest screen in the world which can be seen by billions of people.

For more information on E-safety please visit, www.thinkuknow.co.uk/parents

CORE E-Safety Policy	
Publication Date: Summer 2020	**Owner:** Head of HR