E-SAFETY POLICY

REVIEW DATE	**AUGUST 2019**
NEXT REVIEW	**AUGUST 2020**
NEXT REVIEW	**AUGUST 2021**

1. Summary

The E-Safety Policy (Education) has been created to ensure that children and young people are able to use the internet and related communication technologies as part of the wider duty of care to which all who work in education are bound. In addition, this policy enables staff to identify and manage risks, safeguard and support staff, student and parents/Carers by promoting the safe use of technology.

Keeping Children Safe in Education (2016) outlines the responsibility that schools and the Designated Safeguarding Lead (DSL) have in ensuring that all students, young people and staff use electronic technologies in a safe and productive way. Technology is advancing quickly and can be sued in a beneficial and positive way to educate and develop the young people we work with. However, measures must be taken and procedures and processes followed to ensure the safeguarding of all young people who use this technology. In addition, technology and social media play an important part in the social development and learning of young people, it is the DSL's responsibility to ensure leaders, managers and staff are fully aware of statutory updates and requirements to ensure the safeguarding of young people. The DSL is also responsible for the delivery of information. Advice and Guidance for young people and parents/carers so that they are informed and empowered to use technology and social media in a safe way, and that they know that they can disclose concerns, particularly surrounding grooming, CSE sexting, sexting, the sharing of illicit images and online bullying, in a safe and confident way. This policy is intended to be used in conjunction with the Take 1 Safeguarding Children and young People Policy (whole school).

1. What is the policy about?

The purpose of this Online Safety Policy is to:

- Clearly identify the key principles expected of all members of Take 1's Education community with regards to the safe and responsible use of technology to ensure that the School is a safe and secure environment.
- Safeguard and protect all members of the Take 1 education community online.
- Raise awareness with all members of the Take 1 education community regarding potential risks as well as benefits of technology.
- To enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.

2. Who is the policy for?

This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for or provide services on behalf of Take 1 (collectively referred to as 'staff' in this policy) as well as young people and parents/carers.

3. Policy statement and requirements

3.1 Making use of ICT and the Internet in School

The Internet is used in school to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management functions. Technology is advancing rapidly and is now a huge part of everyday life, education and business. We want to equip our students with all necessary ICT skills that they will need in order to enable them to progress confidently in their educational careers and onward towards their working environments when they leave school. Some of the benefits of using ICT and the internet in schools are:

For students:

- unlimited access to worldwide educational resources and institutions such as art galleries, museums and libraries
- contact with schools in other countries resulting in cultural exchanges between students all over the world
- access to subject experts, role models, inspirational people and organisations. The internet can provide a great opportunity for students to interact with people that they otherwise would never be able to meet
- an enhanced curriculum; interactive learning tools; collaboration, locally, nationally, and globally
- self-evaluation; feedback and assessment; updates on current affairs as they happen
- access to learning whenever and wherever convenient
- freedom to be creative
- freedom to explore the world and its cultures from within a classroom
- social inclusion, in class and online
- access to case studies, videos and interactive media to enhance understanding
- individualised access to learning.

For staff:

- professional development through access to national developments, educational materials and examples of effective curriculum practice and classroom strategies
- immediate professional and personal support through networks and associations
- improved access to technical support
- ability to provide immediate feedback to students and parents
- class management, attendance records, assessment and assignment tracking.

For parents:

- Communication between the school and parents/carers may be through school e-mail and telephone messages. This form of contact can often be considered to be more effective, reliable and economic. Text messages and letters will also inform parent/carers of details relating to attendance, behaviour and other appropriate matters.

a. Roles and Responsibilities:

The School Online-Safety Coordinators are:
Technical: Gavin Gordon IT

Safeguarding: DSL Courtney Rose 07967 032108 and Deputy DSL Naomi Fearon 07908 391676

The Designated Member of the Governing Body Responsible for E-Safety is: Ruthba Choudhury

The role of the Governors:
Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. They receive regular information about online-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor, duties of which will include:

- Regular monitoring of online-safety incident logs
- Regular monitoring of filtering/change control logs

The Role of the Headteacher and Senior Management :

have a duty of care for ensuring the E-Safety of members of the school community, although the day to day responsibility will be delegated to the E-Safety Co-ordinator(s).

- are aware of the procedures to be followed in the event of a serious E-Safety allegation being made against a member of staff.
- are responsible for ensuring that the E-Safety Co-ordinators and all other members of staff receive suitable training to enable them to carry out their E-Safety roles (usually LSCB DSL training).
- will receive, as appropriate, monitoring reports from the E-Safety Co-ordinator.

The Role of the E-Safety Co-ordinator (who is normally a DSL, see below):

- has day-to-day responsibility for E-Safety issues and has a leading role in establishing and reviewing the school E-Safety policies and documents
- 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 advice for staff, as required and advises young people and parents/carers on E-safety and how to staff safe.
- liaises with the Local Authority through the completion of the Annual E-Safety Audit Tool and similar safeguarding audits when required.
- receives reports of E-Safety incidents and creates a log of incidents to inform future developments (following Take 1's Safeguarding reporting procedures)
- reports regularly to the Senior LeadershipTeam

The Role of Technical Staff:

- ensure that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- ensure that the school meets required safety technical requirements and any Local Authority E-Safety Guidance that may apply
- ensure that users may only access the networks and devices through a properly enforced password protection policy in which passwords are regularly changed
- ensure that the filtering policy is applied
- ensure that they keep up to date with E-Safety technical information in order to effectively carry out their E-Safety role and to inform and update others, as appropriate
- ensure that the use of the network / internet / Virtual Learning Environment / remote access / e-mail and software systems are regularly monitored in order that any misuse or attempted misuse can be reported.

The Role of Teaching and Support Staff:

- have an up to date awareness of E-Safety matters from the DSL and the current school E-Safety policy and practices
- have read, understood and signed the Staff Acceptable Use Agreement (AUA)
- report any suspected misuse or problem to the Headteacher and E–Safety Co-ordinator (DSL) for investigation
- ensure that all digital communications with students/ parents/ carers should be on a professional level and only carried out using school systems
- embed E-Safety in all aspects of the curriculum and other activities
- ensure students understand and follow the E-Safety and Acceptable Use Agreements
- ensure students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities and implement current policies with regard to these devices
- ensure that where internet use is pre-planned, students are guided to sites that have been checked as suitable and that processes are in place for dealing with any unsuitable material that is found in internet searches

The Role of the Designated Safeguarding Lead(s):

- To receive appropriate training (through the Local Children's Safeguarding Board) on E-Safety issues and be aware of the potential serious safeguarding/ child protection issues to arise from:
- The sharing of personal data
- Access to illegal/ inappropriate materials
- Inappropriate on-line contact with adults/ strangers
- Potential or actual incidents of grooming
- Cyber-bullying
- Sexting and the sending of inappropriate images including self-images
- **N.B. It is important to emphasise that these are Child Protection and Safeguarding issues, not simply technical issues i.e.; the technology provides additional means for Child Protection issues to develop.**

The Role of Students and Young People:

- are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Agreement 7
-

- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know, understand and comply with policies on the use of mobile devices and digital cameras
- will be expected to know, understand and comply with policies on the taking/ use of images, sexting 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 covers their actions out of school, if related to their membership of the school.

The Role of Parents/Carers:

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The school will take every opportunity to help parents/carers understand these issues through home/school liaison. Parents and carers will be encouraged to support the school in promoting good E-Safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school
- their children's personal devices in the school

b. Communicating School Policy:

-

This policy is available from the school office and on the school website for parents/carers and staff. Rules relating to the school code of conduct when online and E-Safety guidelines are displayed around the school. E-Safety is integrated into the curriculum where the internet or technology are being used and during PSHEE (Votes for Schools) lessons where personal safety, responsibility, and/or development are being discussed. Parents and carers play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. We will therefore seek to provide information and awareness to parents and carers through curriculum activities and high profile events and campaigns e.g. E-Safety Day.

A link to the CEOP web page will be placed on the school website.

4.4. Training:

Staff:

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy and on the Training Matrix. Training will be offered as follows:

- annual e-safety training from the DSL and through LSCB training.
- all new staff will receive E-Safety training as part of their induction ensuring that they fully understand the school E-Safety policy and Acceptable Use Agreements
- the E-Safety Co-ordinator(s) (DSL(s)) will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations
- this E-Safety Policy and its updates will be presented to and discussed by staff, as appropriate, on INSET days and in meetings
- the E-Safety Co-ordinator(s) (DSL(s)) will provide advice/ guidance/ training to individuals, as required

Governors:

- Governors will be invited to take part in E-safety training / awareness sessions with particular importance for those who are members of any committee involved in technology, e-safety, health and safety and safeguarding / child protection. This may be offered in a number of ways:
- • attendance at training provided by the Local Authority / National Governors Association / or other relevant organisations
- • participation in school training/ information session for staff or parents

4.5. Learning to evaluate Internet Content

- With so much information available online it is important that students learn how to evaluate internet content for accuracy and intent. This is approached by the school as part of digital literacy across the curriculum. Students will be taught:
- to be critically aware of materials they read, and shown how to validate information before accepting it as accurate
- to use age-appropriate tools to search for information online
- to acknowledge the source of information used and to respect copyright. Plagiarism is against the law and the school will take any intentional acts of plagiary very seriously; for students who are found to have plagiarised, appropriate action will be taken

The school will also take steps to filter internet content to ensure that it is appropriate to the age and maturity of students. If staff or students discover unsuitable sites then the URL will be reported to the school E-Safety Co-ordinator (DSL). Any material found by members of the school community that is believed to be unlawful will be reported in accordance with policies and procedures. Regular software and broadband checks will take place to ensure that filtering services are working effectively.

4.6. Managing Information Systems

The school is responsible for reviewing and managing the security of the computers and internet networks as a whole and takes the protection of school data and personal protection of our school community very seriously. This means protecting the school network, as far as is practicably possible, against viruses, hackers and other external security threats. The security of the school information systems and users will be reviewed regularly by the Network Manager and virus protection software will be updated regularly. Some safeguards that the school takes to secure our computer systems are:

- ensuring that all personal data sent over the internet or taken off site is encrypted/ password protected
- ensuring that unapproved software is not downloaded to any school computers;
- files held on the school network will be regularly checked for viruses
- the use of user logins and passwords to access the school network will be enforced portable media containing school data or programmes will not be taken off-site without specific permission from a member of the senior leadership team
- Regular reporting to Governors
- For more information on data protection in school, please refer to the Take 1 Data Protection policy. More information on protecting personal data can be found in Section 3.12 of this policy.

4.7. E-mail

The school uses email internally for staff and externally, for contacting parents. It is an essential part of school communication. It is also used to enhance the curriculum by initiating contact and projects with other schools nationally and internationally. It may also be used to provide immediate feedback on work and requests for support where it is needed. Staff and students should be aware that school email accounts should only be used for school-related matters, i.e.; for staff to contact parents, students, other members of staff and other professionals for work purposes. This is important for confidentiality. The school has the right to monitor emails and their content but will only do so if it feels there is reason to.

4.8.School Email Accounts and Appropriate Use

- Staff should be aware of the following when using email in school:

- staff should only use official school-provided email accounts to communicate with students, parents or carers; personal email accounts should not be used to contact any of these people for school business
- emails sent from school accounts should be professionally and carefully written; staff are representing the school at all times and should take this into account when entering into any communication
- staff must tell their Manager or a member of the Senior Leadership Team if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account; they should not attempt to deal with this themselves
- the forwarding of chain messages is not permitted in school.

Students should be aware of the following when using email in school:

- Take 1 does not issue student email accounts.
- they will be educated through the ICT curriculum to identify spam, phishing and virus emails and attachments that could cause harm to the school network or their personal wellbeing.

4.8.1. Published Content and the School Website

The school website is viewed as a useful tool for communicating our school ethos and practice to the wider community. It is also a valuable resource for parents/carers and students by providing information. The website is in the public domain, and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the school community, copyrights and privacy policies. No personal information on staff or students will be published, and details for contacting the school will be for the school office only. For information on the school policy on students' photographs on the school website please refer to section 3.8.2 of this policy.

4.8.2 Policy and guidance of safe use of student's photographs and work

Take 1 believes that celebrating the achievement of children and young people in school is an important part of their learning experience and personal development. Taking photographs and videos of students for internal display and displaying student work for educational use enables us to celebrate individual and group successes as a school community.

Colour photographs and students' work bring our school to life, showcase our students' talents and add interest to school publications both online and in print. However, the school has safety precautions in place to prevent the misuse of such material:

Photographs, images and videos of the school and students will only be used in accordance with the Data Protection Act 1998 and with prior parental/carer consent, as outlined in the Home/School Agreement which is drawn up on admission to the school. On admission, parents/carers will also be asked to sign an Acceptable Use Agreement which incorporates digital/video permissions.

By signing this form parents/carers will be consenting to the use of images of their child being used in the following outlets:

- all school and Take 1 publications
- on the school website
- in newspapers as allowed by the school
- in videos made by the school or in class for school projects

The consent lasts for the duration of the student's time at the school. Once the pupil leaves the school, photographs and videos may be archived within the school but will not be re-published without renewed consent. In circumstances where the student is aged 18 or above, personal consent will be required from the student in addition to parental authorisation.

Student's full names will never be published externally with their photographs, but may be published internally (for example, on display with their work).

Using photographs of individual students:
Students may not be approached about being photographed while in school or engaging in school activities without the school's permission. The school follows these general rules on the use of photographs of individual students:

- Parental consent must be obtained for external/promotional use- see above.
- Electronic and paper images will be stored securely.
- Images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that photographs are appropriate for the public domain.
- For public documents, including in newspapers, full names will not be published alongside images of the child. Groups may be referred to collectively by year group or form name.
- Parents/ carers are not permitted to take photographs or videos whilst on the school premises.
- Students are encouraged to tell a member staff if they are concerned or uncomfortable with any photographs that are taken of them or events they are being asked to participate in.
- Any official photographers that are commissioned by the school will be fully briefed on Child Protection matters in relation to their work, will wear identification at all times, and will not have unsupervised access to students at any time.

4.8.3 Complaints of misuse of photographs or video
Parents/ carers should follow the standard Take 1 complaints procedure if they have a concern or complaint regarding the misuse of school photographs.

4.8.4 Social networking, social media and personal publishing
The school follows the following rules on the use of social media and social networking sites in school:
• Students are educated on the dangers of social networking sites and how to use them in safe and productive ways. They are all made fully aware of the school's code of conduct regarding the use of ICT and technologies and behaviour online including sexting. This is delivered through PSHEe lessons and the delivery of Votes for Schools.
• Any sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.

• Official school blogs created by staff or students/year groups/school clubs as part of the school curriculum will be password-protected and run with the approval of a member of staff and will be moderated by a member of staff.
• Students and staff are not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The school expects all staff and students to remember that they are representing the school at all times and must act appropriately.
• Safe and professional behaviour of staff online will be discussed during the staff induction process.

4.9. Mobile Phones and Personal Devices

While mobile phones and personal communication devices are common place in today's society, their use and the responsibility for using them should not be taken lightly. Some issues surrounding the possession of these devices are:
• they can make students and staff more vulnerable to cyberbullying
• they can be used to access inappropriate internet material
• they can be a distraction in the classroom
• they are valuable items that could be stolen, damaged, or lost
• they can have integrated cameras, which can lead to child protection, bullying and data protection issues, including the sharing of inappropriate or illicit images and sexting.

The school adopts a zero tolerance policy in relation to electronic devices owned by students and brought onto school premises in relation to the making and distribution of images and/ or recordings of students and staff.

We do however; understand that a parent/carer may wish for their child to have a mobile phone for their journey to and from school. In this situation a student should adhere to the following procedure:

Emergencies:
• If a student needs to contact his parents/carers, a school phone will be made available.
• If parents/carers need to contact their child urgently they should phone the school office and a message will be relayed promptly.

Responsibility:
• Take 1 accepts no responsibility whatsoever for theft, loss or damage relating to phones/devices including those handed in.
• Take 1 will not investigate the theft, loss or damage relating to student phones/devices.

Staff
• Under no circumstances should staff use their own personal devices to contact students or parents either in or out of school time unless in an emergency.
• Staff are not permitted to take photos or videos of students on personal devices. If photos or videos are being taken as part of the school curriculum or for a professional capacity, the school equipment will be used for this.
• The school expects staff will lead by example: Personal mobile phones will be switched off or placed on ‘silent’ and stored away in a safe location during school hours.

• Any breach of school policy may result in disciplinary action being taken against that member of staff.

4.10. Cyberbullying
Cyberbullying, as with any other form of bullying, is taken very seriously by the school. If an allegation of bullying does come up, the school will:
• take it seriously
• act as quickly as possible to establish the facts. It may be necessary to examine school systems and logs or contact the service provider in order to identify the perpetrator.
• record and report the incident
• provide support and reassurance to the victim
• make it clear to the perpetrator that this behaviour will not be tolerated. Appropriate action will be taken, as necessary.
• Follow the Anti-Bullying Procedure.

4.11. Managing Emerging Technologies
Technology is progressing rapidly and new technologies are emerging all the time. The school will risk-assess any new technologies before they are allowed in school, and will consider any educational benefits that they might have. The school keeps up-to-date with new technologies and is prepared to quickly develop appropriate strategies for dealing with new technological developments.

4.12. Protecting Personal Data
Take 1 believe that protecting the privacy of our staff and students and regulating their safety through data management, control and evaluation is vital to whole-school and individual progress. The school collects personal data from students, parents, and staff and processes it in order to support teaching and learning, monitor and report on student and teacher progress, and strengthen our pastoral provision.

We take responsibility for ensuring that any data that we collect and process is used correctly and only as is necessary, for full and comprehensive information on how the school safeguards data, refer to the Take 1 Data Protection policy.

4.13. Unsuitable/ inappropriate activities:
Any of the following activities are deemed inappropriate in school:
• the accessing of pornography
• the promotion of any kind of discrimination

• the use of threatening behaviour, including promotion of physical violence or mental harm
• using any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute
• using school systems to run a private business
• using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school
• infringing copyright
• revealing or publicising confidential or proprietary information e.g. financial, personal information, data bases, computer / network access codes and passwords
• creating or propagating computer viruses or other harmful files
• unfair usage
• on-line gaming, educational and non-educational
• on-line gambling
• the use of social media without permission
• the use of messaging apps without permission
• the use of videoing broadcasting or YouTube without permission

4.14. Responding to Incidents of Misuse
Managers should refer to the Take 1 Data Protection Policy, Take 1 Safeguarding Children and Young People Policy and the Take 1 Staff Code of Conduct.

Illegal incidents
If there is any suspicion that the website(s) concerned may contain child abuse images, or if there is any other suspected illegal activity Take 1 reporting procedures should be followed as outlined in the Take 1 Safeguarding Children and Young People policy.

Other incidents
It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow Take 1 policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:
• More than one senior member of staff should be involved in the process and the incident reported following the Take 1 Safeguarding Children and Young People Policy. This is vital to protect individuals if accusations are subsequently reported.

• The procedure should be conducted using a designated computer that will not be used by students and if necessary can be taken off site by the police should the need arise. The same computer should be used for the duration of the process.
• Relevant staff should have appropriate internet access to conduct the procedure, and sites and content visited closely monitored and recorded to provide further protection.
• The ULR of any site containing the alleged misuse and the nature of the content causing concern should be recorded. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. This may be printed, signed and attached to the form (except in cases of child sexual abuse).
• Once fully investigated the group should judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following;
-Internal response or discipline procedures
-Involvement by Local Authority or national/ local organisations (as appropriate)
-Police involvement and/ or action
If content being reviewed includes images of child abuse then the matter should referred to the Police immediately. Other instances to report to the police would include:
• incidents of 'grooming' behaviour
• the sending of obscene materials to a child and from child to child.
• the inclusion of adult material which potentially breaches the Obscene Publications Act
• criminally racist material
• other criminal conduct, activity or material
Isolate the computer in question as best you can. Any changes to its state may hinder a later police investigation.
It is important that all of the above steps are taken as they will provide an evidence trail for the school and the police and demonstrate that visits to these sites were carried out for child protection purposes.

School Actions and Sanctions
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 an appropriate 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 Take 1 behaviour/ disciplinary procedures and could include:

Students:
• Referral to class teacher / tutor
• Referral to E-Safety Co-ordinator(s)
• Referral to Line Manager
• Referral to Headteacher
• Referral to the Police
• Referral to Technical Support staff for action re filtering/ security etc.
• Informing parents / carers
• Removal of network / internet access rights
• Revised Risk Assessment
• Issue of a Warning
• Detention or sanction
• Fixed Term Exclusion
• Permanent Exclusion

Staff:
• Referral to Line Manager
• Referral to Headteacher
• Referral to Local Authority/ HR
• Referral to Line Manager
• Referral to Technical Support staff for action re filtering etc.
• Enhanced Risk Assessment
• Warning
• Referral to agency/ counselling
• Suspension from duty
• Disciplinary action
• Referral to the Police
• Dismissal

5. Related policies

This policy must be read in conjunction with Keeping Children Safe in Education (2016) and other relevant school policies including (but not limited to) Take 1 Safeguarding of Children and Young People Policy, Anti-bullying Policy, Behaviour Policy, Photographic Image Use, Acceptable Use Policies, confidentiality, screening and searching and Take 1 Data Management and Protection Policy. In addition, it relates to the delivery of PSHE, SMSC and IT.