Schools - Online Safety Policy

Accepted by: Board of Directors July 2018
Approving Body : Board of Directors
Committee : Standards
Review Cycle: 1 year
Last reviewed: March 2023
Date for next review: October 2023

1. Introduction

1.1 At Inicio Academies we are working with the Directors, Staff, Pupils and Parents/ Carers to create a school community which:

- Values the use of new technologies in enhancing learning.
- Encourages responsible use of ICT.
- Follows agreed policies to minimise potential Online Safety risks.

2. Rationale

2.1 We aim as a Trust to hit the DFE recommendations that: ***"An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate".*** The so-called 'new' technologies are central to both our lives and those of children and young people in today's society, both in school and outside.

2.2 Electronic communication helps teachers and pupils learn from each other and the wider world, and the technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people have an entitlement to safe Online access at all times.

2.3 The requirement to ensure that children and young people are able to use the Online and related communications technologies appropriately and safely is a part of the wider duty of care by which all who work in schools are bound. It is important for the school to protect pupils and staff alike from the following issues within school:

"The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- *Content: being exposed to illegal, inappropriate or harmful material;*
- *Contact: being subjected to harmful online interaction with other users; and*
- *Conduct: personal online behaviour that increases the likelihood of, or causes, harm".*
- *Commerce:* risks such as online gambling, inappropriate advertising, phishing and financial scams.

2.4 We recognise that the continuing development and implementation of this strategy must involve all the stakeholders in a child's education from the Head Teacher/Head of School and Directors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves if it is to be successful.

2.5 The use of new technologies in school and at home has been shown to raise educational standards and promote pupil achievement. We recognise that the Online and other digital and information technologies are powerful tools, which open up new opportunities for everyone. But these opportunities are not without risk.

2.6 Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the Online
- The risk of being subject to radicalisation
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / Online games
- An inability to evaluate the quality, accuracy and relevance of information on the Online
- 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
- Having a negative effect on their digital footprint, which could affect them in later life.

2.7 Many of these risks reflect situations in the off-line world and it is essential that this Online Safety Policy is seen and understood to operate in conjunction with other school policies, especially the Anti-bullying and Safeguarding Policies all of which can be viewed on individual school websites or at https://swiftacademies.org.uk/policies

2.8 As with all other risks, it is impossible to eliminate these 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.

2.9 We recognise that we must provide the necessary safeguards to help ensure we have done everything that could reasonably be expected in order to manage and reduce these risks. Our Online Safety Policy explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the Online and other communications technologies for educational, personal and recreational use.

3. Scope of the Policy

3.1 This Policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems.

3.2 The school will deal with Online Safety incidents and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online behaviour.

3.3 Help and advice can be provided to Parents by the school via the school website Online Safety tab where links to:

CEOPS www.ceop.police.uk,
twitter.com/ceopuk and
www.ceop.police.uk/safety-centre,
Childline www.childline.org.uk,
www.thinkuknow.co.uk,
Online Watch Foundation www.iwf.org.uk and
How to get safe online www.getsafeonline.org are all available.

3.4 This will help pupils and parents alike to stay safe online and inform them of how to report incidents when they have happened outside of school time on personal devices, through personal accounts.

3.3 The DFE also states through the Keeping Children Safe (2021) document that the following websites can also provide support and advice:
www.thinkuknow.co.uk
www.disrespectnobody.co.uk
www.saferOnline.org.uk
www.Onlinematters.org
www.childnet.com/cyberbullying-guidance
www.pshe-association.org.uk
www.educateagainsthate.com
www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation

UKSafer Online Centre-to report and remove harmful online content and guides and resources

Commonsensemedia-provides independent reviews about all types of media

4. Roles and Responsibilities

4.1 The following section outlines the roles and responsibilities for Online Safety of individuals and groups within the school.

4.2 Directors:

4.2.1 A specified member of the Board of Directors should take on the role of Online Safety link director. The role of the Online Safety Director will include:

- Regular meetings with the Online Safety Co-ordinator / Officer
- Reporting to relevant Directors/LGB committees / meetings

4.3 Head Teacher/Head of School and Senior Leaders:

- The Head Teacher/Head of School is responsible for ensuring the safety (including online Safety) of members of the school community, though the day-to-day

responsibility for online safety will be delegated to the Online Safety Coordinator / Officer

- The Head Teacher/Head of School/Senior Leaders are responsible for ensuring that the Online Safety Coordinator/Officer and other relevant staff receive suitable CPD, which is integrated as a whole school approach, to enable them to carry out their Online Safety roles and to train other colleagues, as relevant.
- The Head Teacher/Head of School/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Head Teacher/Head of School and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious Online Safety allegation being made against a member of staff.

4.4 E-Safety Coordinator/Officer:

- Hurworth School has named members of staff with a day-to-day responsibility for E-Safety: Kelly Davidson
- Longfield School has named members of staff with a day-to-day responsibility for E-Safety: Claire Howlett and Rebecca Wheatley
- The Rydal School has named members of staff with a day-to-day responsibility for E-Safety: Marcus Dickinson, Amy Waller

4.4.1 These people:

- Lead on Online Safety matters in school
- Take day to day responsibility for Online Safety issues and have a leading role in establishing and reviewing the school Online Safety Policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place
- Provide training and advice for staff in cooperation with Safeguarding officers in school Liaise with the Local Authority where appropriate and necessary
- Liaise with Trust ICT technical staff
- Receive reports of Online Safety incidents and create and keep a log of incidents to inform future Online Safety development
- Meet regularly with Online Safety Director to discuss current issues, review incident logs and filtering / change control logs
- Attend relevant meeting/committee of LGB/ Directors
- Will provide a report that will illustrate any Online Safety issues and trends that may be occurring within school.

4.5 Incidents that infringe the Online Safety Policy will be dealt with according to their severity.

4.6 The investigation / action / sanctions in case of pupil infringement of the policy will be dealt with via the school systems outlined in the policy, but any major incident or incidents involving any employee or parent/carer or community user must be reported immediately to the Online Safety Coordinator/Officer, Head of Pastoral Care or the Head Teacher/Head of School.

4.7 In the case of pupils, the full range of school sanctions are open to the Head Teacher/Head of School for deliberate infringement of the Policy, up to and including fixed term or permanent exclusion. If an incident has occurred outside of school then a full range of

support/ advice is provided to parents about actions that should be taken and where to report incidents or seek advice (please refer to the scope of the Policy section).

4.8 In the case of staff, the full range of disciplinary responses are open to the Head Teacher/Head of School for deliberate infringement of the Policy, up to and including recommending dismissal.

4.9 In the case of infringement by Parents/Carers or community users the Head Teacher/Head of School will refer the matter to the appropriate external agency, for example Social Services or the police.

4.10 Schools ICT Manager and Technical staff:

4.10.1 The Schools ICT Manager is responsible for ensuring:

- That the school's IT infrastructure is secure and is not open to misuse or malicious attack
- That the school meets the Online Safety technical requirements
- That users may only access the school's networks through a properly enforced password protection policy as outlined in the IT Acceptable User Policy
- The school's filtering system, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- They keep up to date with Online Safety technical information in order to effectively carry out their Online Safety role and to inform and update others as relevant
- That the use of the network / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Online Safety Coordinator for investigation / action / sanction
- That monitoring software / systems are implemented and updated as agreed in school policies

4.11 Teaching and Support Staff

4.11.1 Staff training is provided on Safeguarding & Online Safety in accordance with the latest guidance contained in the DfE's Keeping Children Safe in Education.

4.12.2 Teaching and Support Staff are responsible for ensuring that:

- They have an up-to-date awareness of Online Safety matters and of the current school Online Safety Policy and practices
- They have read, understood the school Policy on use of ICT (IT Acceptable User Policy)
- They report any suspected misuse or problem to the Online Safety Coordinator for investigation / action / sanction
- Digital communications with pupils should be on a professional level and only carried out using official school systems
- Online Safety issues are embedded in all aspects of the curriculum and other school activities
- Staff understand and follow the school Online Safety and IT Acceptable User Policy
- Staff have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They are aware of Online Safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices

- In lessons where Online 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 Online searches
- Staff understand how and where to report any incidents, worries or concerns regarding Online Safety and can give advice to pupils surrounding this.

4.13 Designated Person for Child Protection

4.13.1 Designated Child Protection trained staff must be trained in Online Safety issues and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Cyber-bullying
- Accessing extremist materials

4.13.2 When dealing with an incident involving nude/semi nude images, Pastoral staff should follow this guidance:

https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-educationsettings-working-with-children-and-young-people/sharing-nudes-and-semi-nudes-advice-for-educationsettingshttps://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-peopleworking-with-children-and-young-people

4.14 Pupils:

- Are responsible for using the school ICT systems in accordance with the IT Acceptable User Policy, which they electronically accept on entry to the school internet/ network
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber- bullying
- Should understand the importance of adopting good Online Safety practice when using digital technologies out of school.

4.15 Parents/Carers:

4.15.1 Parents/carers play a crucial role in ensuring that their children understand the need to use the online / mobile devices in an appropriate way.

4.15.2 Parents and carers will be responsible for:

- Accessing the school website / on-line pupil records in accordance with the relevant school IT Acceptable User Policy

4.16 Community Users

4.16.1 Community Users who access school ICT systems / website as part of the Extended School provision will be expected to sign **Acceptable User Policy. This will also apply to temporary members of teaching staff. The Schools ICT Manager will hold a register of users. In addition, all users will have to agree to the policy electronically on entrance to the school ICT network.**

4.17 Education of pupils

4.17.1 We believe that whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in Online Safety is therefore an essential part of our school's Online Safety provision. Children and young people need the help and support of the school to recognise and avoid Online Safety risks and build their resilience.

4.17.2 Online Safety education will be provided in the following ways:

- A planned Online Safety programme is provided
- Key Online Safety messages are reinforced as part of a planned programme of assemblies and tutorial / PSHE and pastoral activities
- Pupils are explicitly taught in all lessons to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information
- Pupils are helped to understand the need for the IT Acceptable User Policy and encouraged to adopt safe and responsible use of ICT, internet and mobile devices both in and outside school
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Online
- Staff are expected to act as good role models in their use of ICT, Online and mobile devices
- Online rules will be posted in all rooms
- Online Safety week provides many activities and materials to educate the pupils on the importance of Online safety issues.

4.18 Education – Parents/Carers

4.18.1 Many parents and carers have only a limited understanding of Online Safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences.

4.18.2 Parents often underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material online and are often unsure about what they would do about it. Parents also sometimes find it difficult to know which Apps or websites their children are accessing and using.

"There is a generational digital divide". (Byron Report).

4.18.3 The school provides information and awareness to parents and carers through:

- Parental Online Safety awareness information & sessions
- Website – which provides parents/carers with help and support with how to educate pupils, how to report incidents and how to educate themselves

4.19 Education and Training – Staff

4.19.1 We regard it as essential that all staff receive Online Safety training and understand their responsibilities, as outlined in this Policy. Training will be offered as follows:

- It is expected that some staff will identify Online Safety as a training need within the Appraisal process
- All new staff will receive Online Safety training as part of their induction programme via their safeguarding briefing and awareness session (NQT / New staff induction programme), ensuring that they fully understand the school's Online Safety Policy and IT Acceptable User Policy
- The Online Safety Coordinator/Officer should receive regular updates through attendance at LA and other information / training sessions and by reviewing any guidance documents
- The Online Safety Coordinator/Officer (or other nominated person) will provide advice / guidance / training as required to individuals as required.

4.20 Training – Directors

4.20.1 Directors should take part in Online Safety training / awareness sessions, with particular importance for those who are members of any sub-committee / group involved in ICT / Online Safety / Health and Safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/National Directors Association or other relevant organisation
- Participation in school training / information sessions for staff or parents
- Technical – infrastructure / equipment, filtering and monitoring

4.21 Responsibility of the School

- The school will be responsible for ensuring that the school infrastructure/ network is as safe and secure as is reasonably possible and that policies and procedures approved within this Policy are implemented
- School ICT systems will be managed in ways that ensure that the school meets the Online Safety technical requirements outlined in any relevant Online Safety Policy and guidance.
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Schools IT Manager
- All users will be provided with a username and password by the Schools ICT Manager or nominated member of the Network Team. The Schools ICT Manager will keep an up-to-date record of users and their usernames
- The "master / administrator" passwords for the school ICT system, used by the Schools ICT Manager must also be available to the Head Teacher/Head of School or other nominated Senior Leader and kept in a secure place (e.g. school safe)
- Users are responsible for the security of their username and password, and must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
- The school has provided enhanced user-level filtering

- In the event of the Schools ICT Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Head Teacher/Head of School (or other nominated Senior Leader)
- Requests from staff for sites to be removed from the filtered list will be considered by the Schools ICT Manager and Online Safety Co-ordinator. If the request is agreed, this action will be recorded
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the IT Acceptable User Policy
- Remote management tools are used by staff to control workstations and view users' activities
- The school discipline system shall be used for users to report any actual / potential Online Safety incident to the Online Safety Co-ordinator /Schools ICT Manager when this occurs in school time
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data
- An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the school system
- An agreed policy is in place regarding the extent of personal use that users (staff/students/pupils/ community users) and their family members are allowed on laptops and other portable devices that may be used out of school. This is administered and held by the Schools ICT Manager
- The school infrastructure and individual workstations are protected by up-to-date virus software
- Personal data must not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured and with the permission of the Online Safety Co-ordinator
- To provide parents, staff and pupils alike on where to gain advice and help on Online Safety issues.

5. Curriculum

5.1 Online Safety is a focus in all areas of the curriculum and staff are expected to reinforce Online Safety messages in the use of ICT across the curriculum.

- In lessons where Online use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use
- Where pupils are allowed to freely search Online, e.g. using search engines, staff are expected to be vigilant in monitoring the content of the websites the young people visit. Where installed, staff will be expected to monitor pupil's activity using the Impero system installed in all ICT rooms
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in online searches being blocked.
  In such a situation, staff can request that the Schools ICT Manager can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need
- Pupils are taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

5.2 The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images online.

5.3 Those images may remain available online forever and may cause harm or embarrassment to individuals in the short or longer term.

5.4 There are many reported incidents of employers carrying out online searches for information about potential and existing employees. The school informs and educates users about these risks and implements policies to reduce the likelihood of the potential for harm:

- When using digital images, staff inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, pupils are taught to recognise the risks attached to publishing their own images online e.g. on social networking sites
- Staff are allowed to take digital / video images to support educational aims, but must follow the school policy concerning the sharing, distribution and publication of those images
- Those images should only be taken on school equipment; personal equipment of staff should not be used for such purposes
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images
- Written permission from parents/carers will be obtained before photographs of pupils are published on the school website
- Pupil's work can only be published with the permission of the pupil and parents/ carers

6. Data Protection

6.1 Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation 2018 which states that personal data must be:

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

6.2 Staff must ensure that they:

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

7. Dealing with breaches of the Policy

7.1 Any use that contravenes this policy will be dealt with by the standard disciplinary routes and may involve withdrawal of ICT usage privileges and potential disciplinary action. These sanctions will be applied at the discretion of the Head Teacher/Head of School.

7.2 Online Safety incidents involving students will be reported via the normal referral routes. Any incident will then be recorded on CPOMS and tagged as an online safety incident.

Communications

The following table outlines how communication technologies are to be used safely in school:

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times in non-pupil facing areas.	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones/smartwatches may be brought to school		X					To be kept in a secure place	
Use of mobile phones/smartwatches in lessons				X				X
Use of mobile phones/smartwatches in social time	X							X
Taking photos on mobile phones or other camera devices	Only school devices				Only school devices			
Use of personal email addresses in school, or on school network				X				X
Use of school email for personal emails				X				X
Use of school social networking sites e.g twitter and Tapestry	X				X			
Use of instant messaging on school technology				X				X
Use of **personal** social networking sites/chat rooms on school technology				X				X
Use of USB devices	Only with permission from Online coordinator							X