E-SAFETY

POLICY AND PROCEDURE

OCTOBER 2021
(Review Due: October 2024)

INSPIRE SUFFOLK

E-Safety Policy

1 INTRODUCTION

The introduction of the E-Safety Policy is to safeguard and promote the welfare of all members of the Inspire Suffolk community when using technologies both on site and at home. Online safety is an essential part of safeguarding and the charity has a duty to ensure that all students and staff are protected from harm when using mobile technology or social media.

Mobile devices, such as computers, tablets, mobile phones, smart watches and games consoles, and social media, are an important part of everyday life, which present positive and exciting opportunities, as well as challenges and risks. Inspire Suffolk will empower our students to acquire the knowledge needed to use the mobile technology and social media in a safe, considered and respectful way, develop high levels of digital skills and develop their resilience so they can manage and respond to online risks, as well as prepare for future learning opportunities and employment.

The policy takes into account the DfE statutory guidance 'Keeping Children Safe in Education' 2020 procedures and in line with DfE Guidance, 'Safeguarding and remote education during coronavirus (COVID 19)' 2020. The policy reflects the significant shift to blended learning in response to coronavirus where students are asked to undertake remote learning, and may be asked to increase the proportion of learning online at home in response to a full or partial closure.

The policy also takes account of the UKCIS digital resilience framework, 2020 which provides a framework for building resilience in staff and students' digital lives.

2 SCOPE OF THE POLICY

The policy applies to all users; students, staff and all members of the Charity community who have access to the Charity IT systems, both on the premises and remotely, and to those using their personal devices on the premises. The E-Safety Policy applies to all use of the internet and electronic communication devices such as e-mail, mobile phones, games consoles and social networking sites and Apps.

The policy refers primarily to use of technology on Charity premises or for Charity related educational work or through communication channels that specifically link to the Charity. However, this policy may also apply to conduct by students or staff (such as incidents of cyber-bullying or other e-safety incidents covered by this policy) which take place out of Charity, but is linked to membership of the Charity and which impacts on the Charity community, individuals or reputation.

3 RISKS

There are a wide range of risks and dangers that face young people which could impact on the safety or security of students. To help categorise the risks, the policy has adopted the categories identified in Annexe C of Keeping Children in Safe Education 2020. 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 internet;
- The sharing / distribution of personal images without an individual's consent or knowledge;
- Inappropriate communication / contact with others, including strangers, for example through social networking sites;
- Cyber-bullying;
- Race hatred;
- Terrorism extremism;
- Access to unsuitable video / internet games/gambling sites;
- Financial abuse;
- Plagiarism and copyright infringement;
- Illegal downloading of music or video files;
- The potential for use which may impact on the social and emotional development and learning of the young person, increasing their vulnerability through the sharing of personal data which may allow: Access or exposure to illegal / inappropriate materials
- The potential for use which may impact on the social and emotional development and learning of the young person, increasing their vulnerability through the sharing of personal data which may allow: inappropriate on-line contact with adults / strangers; potential or actual incidents of grooming; cyber-bullying
- The potential for use which may impact on the social and emotional development and learning of the young person, increasing their vulnerability through the sharing of personal data which may allow: inappropriate portrayal of self to others

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, to build students' 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.

4 ROLES AND RESPONSIBILITIES

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

Senior Management Team

The Senior Management Team is responsible for ensuring the safety (including e-safety) of members of the Charity community and will take action as is appropriate and necessary. The SMT takes responsibility for e-safety issues and has a leading role in:

- establishing and reviewing the Charity e-safety policies, including procedures that need to be followed in the event of an e-safety incident taking place;

- advises re. staff development;
- liaises with Astute;
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments;

IT Services

Astute (IT Services provider) is responsible for ensuring:

- that the Charity's IT infrastructure is secure and is not open to misuse or malicious attack;
- that users may only access the Charity's networks through a properly enforced password protection policy;
- the Charity's filtering policy is applied and updated on a regular basis;
- that the use of the Charity network remote access and email is logged where appropriate in order that any misuse or attempted misuse can be investigated and reported;

Teaching and Support Staff

All staff are responsible for ensuring that they:

- take responsibility for ensuring that students are e-safety aware;
- take responsibility for the safe use by students of specified technologies which are part of teaching and learning;
- complete training as required by the Charity;
- have an up to date awareness of e-safety matters;
- report any suspected misuse or problem, including incidents of cyberbullying;
- they monitor IT activity; extra-curricular and where appropriate extended Charity activities.

Students

Students are:

- responsible for using the Charity IT and/or communication systems and mobile devices;
- expected to seek help and follow procedures where they are worried or concerned, or where they believe an e-safety incident has taken place involving them or another member of the Charity community;
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- expected to know and understand Charity policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand Charity policies on the taking / use of images and on cyber-bullying;
- expected to understand the importance of adopting good e-safety practice when using digital technologies out of Charity.

5 ACCEPTABLE USE

The Charity will not tolerate any abuse of IT systems. Whether offline or online, communications by staff and students should be courteous and respectful at all times. Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and in line with the disciplinary codes of practice.

Where conduct is found to be unacceptable, the Charity will deal with the matter internally. Where conduct is considered illegal, the Charity will report the matter to the police.

6 COMMUNICATIONS

There are a variety of technologies now available with which individuals can communicate with one another. All digital communications with students must be professional in tone and content at all times.

Staff will:

- ensure that personal e-mail accounts, mobile/home telephone numbers are not shared with students;
- not allow students to add a member of staff as a friend to their social networking site nor will staff add them as friends to their personal social networking site(s);
- ensure that any private social networking sites / blogs etc. that they create or actively contribute to are not confused with their professional role;
- not use personal digital cameras or camera phones for transferring images of children and young people or staff without permission;
- not engage in any online activity that may compromise their professional responsibilities.

7 USE OF IMAGES AND VIDEO

The use of images, or photographs, is popular in teaching and learning and should be encouraged where there is no breach of copyright or other rights of another person. This will include images downloaded from the internet and images belonging to staff or students.

All students and staff should understand the risks in downloading these images as well as posting them online and sharing them with others. There are particular risks where personal images are posted onto social networking sites for example.

Where students wish to take and/or use photographs or videos of students or staff, they must obtain the consent of the individual(s) in advance and be clear about what their intentions are in relation to using the material, ie how they plan to use it. Photographs of activities on the Charity premises should be considered carefully and should not include full names of individuals. Our aim is to reinforce good practice as well as offer further information for all users on how to keep their personal information safe.

8 EDUCATION AND TRAINING

Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the Charity's e-safety provision to help recognise and avoid e-safety risks and build their resilience.

E-Safety education will be provided in the following ways:

- students will be encouraged to adopt safe and responsible use of IT, the internet and mobile devices both within and outside Charity;
- key e-safety messages will be reinforced as part of curriculum delivery which will cover:
- the need to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information;
- acknowledgement of the potentially serious impact of inappropriate use on the Charity and individuals;
- how to report misuse that they observe or are subject to and how to receive appropriate support;
- the need to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

9 SECURITY

The Charity will do all that it can to make sure the Charity network is safe and secure. Every effort will be made to keep security software up to date. Appropriate security measures will include the use of enhanced filtering and protection of firewalls, servers, routers, work stations etc. to prevent accidental or malicious access of Charity systems and information.

Technical infrastructure

- Charity IT systems will be managed in ways that ensure that the Charity meets required e-safety technical requirements.
- There will be regular reviews and audits of the safety and security of Charity IT systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to Charity IT systems.
- All users will be provided with a username and password at enrolment or commencement of employment.
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

Personal Information

Inspire Suffolk collects and stores the personal information of students and staff regularly e.g. names, dates of birth, email addresses, assessment materials and so on. The Charity will keep that information safe and secure in line with GDPR requirements.

Staff must keep students personal information safe and secure at all times and minimise the risk of its loss or misuse. Personal data should only be used on password protected computers and other devices. Every user should ensure that they are properly 'logged off' at the end of any session in which they are using personal data or where they are physically absent, the device should be locked or logged off. When transferring data encryption and secure password protected devices should be used. Any Charity owned mobile device (laptop, USB, mobile phone, ipad or tablet) should be password protected and signed out by the relevant staff member.

10 RESPONDING TO INCIDENTS

It is hoped that all members of the Charity community will be responsible users of IT, 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.

When this occurs staff and students may be subject to disciplinary process. It is the responsibility of staff and students to report any apparent or actual incidents of misuse by students or staff which may include:

- Any behaviour by staff or students which affects the safety and security of the IT systems or other users.
- Any failings in technical safeguards which may become apparent when using the systems and services.
- Any incidents, messages or access to sites that make staff or students feel uncomfortable or unsafe
- Any damage or faults involving equipment or software, however this may have happened.

Misuse by students should be reported to the relevant Tutor/Team Leader/Sports Development Officer and will be dealt with through the Charity Student Performance and Behaviour Policy.

Misuse by staff should be reported to the relevant Line Manager.

Incidents raising safeguarding concerns

Any incidents that raise safeguarding concerns should reported to the designated person or deputy. Where a member of staff is involved in this, a referral to the Local Authority Designated Officer (LADO) should be made.

The following incidents must always be reported to the Police:

- Discovery of indecent images of children and young people.
- Behaviour considered to be 'grooming'.
- Sending of obscene materials.

Incidents involving illegal content

On discovery of illegal content, the equipment or materials found should not be touched.

- Computers or other devices should not be switched off unless it is authorised to do so by the Police.
- Further access to the illegal content should be prevented by keeping other people out of the area.
- If necessary the monitor itself can be turned off but the computer should remain as you have found it (DO NOT shut the machine down).
- If the device is a laptop, do not close as this may cause the machine to power off.
- No attempt should be made to download, print or send any materials found. (By doing so you may commit further offences)
- All illegal content must be reported to the Police and the Internet Watch Foundation (www.iwf.org.uk)

Serious incidents involving electronic media

In the event of a serious incident involving electronic media occurring, it is essential that a review of all E-Safety and Acceptable Use policies and procedures be conducted as soon as possible.

Annex C: Online Safety

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. 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 breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

• **content:** being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;

• **contact:** being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and

• **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

Education

Opportunities to teach safeguarding, including online safety, are discussed at paragraph 88-90. Resources that could support schools and colleges include:
• Be Internet Legends developed by Parent Zone and Google is a free internet safety curriculum with PSHE accredited lesson plans and teaching resources for Key Stage 2 pupils

• Disrespectnobody is Home Office advice and includes resources on healthy relationships, including sexting and pornography

• Education for a connected world framework from the UK Council for Internet Safety supports the development of the curriculum and is of particular relevance to RSHE education and Computing. It is designed, however, to be usable across the curriculum and beyond (covering early years through to age 18) and to be central to a whole school or college approach to safeguarding and online safety.

• PSHE association provides guidance to schools on developing their PSHE curriculum

Teaching online safety in school is departmental guidance outlining how schools can ensure their pupils understand how to stay safe and behave online as part of existing curriculum requirements

• Thinkuknow is the National Crime Agency/CEOPs education programme with age specific resources

• UK Safer Internet Centre developed guidance and resources that can help with the teaching of the online safety component of the Computing Curriculum.

Protecting children

Governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filters and monitoring systems in place.

Whilst considering their responsibility to safeguard and promote the welfare of children, and provide them with a safe environment in which to learn, governing bodies and proprietors should

consider the age range of their pupils, the number of pupils, how often they access the IT system and the proportionality of costs vs risks.
The appropriateness of any filters and monitoring systems are a matter for individual schools and colleges and will be informed in part, by the risk assessment required by the Prevent Duty.

UK Safer Internet Centre has published guidance as to what "appropriate" filtering and monitoring might look like: UK Safer Internet Centre: appropriate filtering and monitoring.

Guidance on e-security is available from the National Education Network. Support for schools is available via the: schools' buying strategy with specific advice on procurement here: buying for schools.

Whilst filtering and monitoring is an important part of the online safety picture for schools and colleges to consider, it is only one part. Governors and proprietors should consider a whole school or college approach to online safety. This will include a clear policy on the use of mobile technology in the school or college. Many children have unlimited and unrestricted access to the internet via 3G, 4G and 5G in particular and the school and college should carefully consider how this is managed on their premises.

Whilst it is essential that governing bodies and proprietors ensure that appropriate filters and monitoring systems are in place, they should be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding.

Reviewing online safety

Technology in this area evolves and changes rapidly. A free online safety self-review tool for schools can be found via the 360 safe website. UKCIS has published Online safety in schools and colleges: Questions for the governing board to help responsible bodies assure themselves that their online safety arraignments are effective.

Education at home
Where children are being asked to learn online at home the department has provided advice to support schools and colleges do so safely: safeguarding-in-schools-colleges and-other-providers and safeguarding-and-remote-education

Staff training

Governors and proprietors should ensure that, as part of the requirement for staff to undergo regularly updated safeguarding training (paragraph 84) and the requirement to ensure children are taught about safeguarding, including online safety (paragraph 87), that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach.

Information and support

There is a wealth of information available to support schools, colleges and parents/carers to keep children safe online. The following list is not exhaustive but should provide a useful starting point:

Advice for governing bodies/proprietors and senior leaders

• Childnet provide guidance for schools on cyberbullying

• Educateagainsthate provides practical advice and support on protecting children from extremism and radicalisation

• London Grid for Learning provides advice on all aspects of a school or college's online safety arrangements

• NSPCC provides advice on all aspects of a school or college's online safety arrangements

• Safer recruitment consortium "guidance for safe working practice", which may help ensure staff behaviour policies are robust and effective

• Searching screening and confiscation is departmental advice for schools on searching children and confiscating items such as mobile phones

• South West Grid for Learning provides advice on all aspects of a school or college's online safety arrangements

• Use of social media for online radicalisation - A briefing note for schools on how social media is used to encourage travel to Syria and Iraq

• UK Council for Internet Safety have provided advice on sexting-in-schools-and colleges and using-external-visitors-to-support-online-safety-education

Remote education, virtual lessons and live streaming

• Case studies on remote education practice are available for schools to learn from each other

• Departmental guidance on safeguarding and remote education including planning remote education strategies and teaching remotely

• London Grid for Learning guidance, including platform specific advice

• National cyber security centre guidance on choosing, configuring and deploying video conferencing

• National cyber security centre guidance on how to set up and use video conferencing

• UK Safer Internet Centre guidance on safe remote learning

Support for children

• Childline for free and confidential advice

• UK Safer Internet Centre to report and remove harmful online content

• CEOP for advice on making a report about online abuse

Parental support

• Childnet offers a toolkit to support parents and carers of children of any age to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support

• Commonsensemedia provide independent reviews, age ratings, & other information about all types of media for children and their parents

• Government advice about protecting children from specific online harms such as child sexual abuse, sexting, and cyberbullying

• Government advice about security and privacy settings, blocking unsuitable content, and parental controls

• Internet Matters provide age-specific online safety checklists, guides on how to set parental controls on a range of devices, and a host of practical tips to help children get the most out of their digital world

• Let's Talk About It provides advice for parents and carers to keep children safe from online radicalisation

• London Grid for Learning provides support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online

• Lucy Faithful! Foundation StopItNow resource can be used by parents and carers who are concerned about someone's behaviour, including children who may be displaying concerning sexual behaviour (not just about online)

• National Crime Agency/CEOP Thinkuknow provides support for parents and carers to keep their children safe online

• Net-aware provides support for parents and carers from the NSPCC and 02, including a guide to social networks, apps and games

• Parentzone provides help for parents and carers on how to keep their children safe online

- Parent info from Parentzone and the National Crime Agency provides support and guidance for parents from leading experts and organisations

• UK Safer Internet Centre provide tips, advice, guides and other resources to help keep children safe online