Document name
E-Safety Policy

This document is relevant to:	
Central Support Services	✓
Education	✓
Medical Therapy	✓
Residential	✓

Senior Manager Responsible	Ellie Crosthwaite (Safeguarding Manager)
Author	Melanie Muir, ICT Group
Superseded Documents	E-Safety Policy (Nov 2015)
Date of Latest Review	Sep 2018
Date of Next Review	Sep 2020
Changes in this revision	Added Keeping children safe in education (KCSIE) Sep 2018 throughout policy
Associated Documents	Data Protection Policy, Safeguarding Policy, Whistle Blowing Policy, Prevent Duty 2015, DfE Keeping children safe in education 2018

Equality Impact Assessment		
Name	Comments	Date
Pam Mason	Approved	15/01/2019

SLT Approval	Approval Date:
✓	Oct 2018
Senior Manager Approval	Approval Date
✓	Sep 2018
Adopted by Governing Body	Adoption Date
✓	07/03/2019

Contents of document

E-Safety Policy

1. Introduction

The purpose of this policy is to safeguard all St. John's learners and promote their welfare through educating and supporting them in the safe use and benefits of Internet, Digital and Mobile Technologies (IDMT).

This policy will ensure that the appropriate action is taken immediately where there is an e-safety concern so that learners are kept safe. The primary concern at all times will be the interests and safety of learners.

It is the duty and responsibility of every member of staff to ensure that they are familiar with the E-Safety Policy. Moreover, it is the duty of every member of staff to report immediately any e-safety concerns about a learner at St. John's. If there is any doubt about whether it is a concern or not, staff must report the issue to the Safeguarding Team to discuss this.

Our approach is to identify and implement reasonable safety measures within St. John's, whilst continuing to provide support and training to staff and learners in identifying and managing risk independently and with confidence wherever IDMT are used.

We aim to achieve this through a combination of security measures, training, guidance and implementation of our policies.

This policy should be read in conjunction with the Data Protection Policy, Safeguarding Policy and Whistle Blowing Policy.

Other legislation and guidance that should be observed in conjunction with this policy include the Prevent Duty 2015 and DfE Keeping children safe in education 2018, specifically Annex C (see Appendix A).

2. Definition

E-safety refers to the protection and safeguarding of children, young people and adults in the digital world. It is about learning to understand and use technologies and the online environment in a safe, positive way whenever or wherever accessed.

E-safety is relevant when using the internet (accessible from computers, laptops, tablets, mobile phones, games consoles and other devices like the iPod Touch and internet connected TV) and other technologies such as Email, text /instant messaging, social networking sites, video broadcasting, and so on.

Some of the dangers the virtual world can pose to children, young people and adults include:

- Exposure to unsuitable materials. For example, violence and explicit content; pornography; life style websites such as pro-anorexia, self-harm, suicide or hate sites.
- Physical danger and sexual abuse. For example, through 'grooming' online by adults (often pretending to be other young people).

- Cyberbullying – persistent bullying via social networking sites, websites, instant messaging and text messages.

- Losing control over (perhaps inappropriate) pictures and videos, which may be uploaded and circulated via social network websites, mobile telephones and video broadcasting websites such as You Tube.

- Obsessive use of IDMTs. For example, addiction to video games.

- Damage to virtual reputation.

- Recruitment by people with extreme political and cultural views which can lead to radicalisation.

- Viruses, hacking and security.

- Copyright infringement. For example, the illegal sharing of music, pictures, video documents.

3. Implementation

3.1 Staff Training

Training in e-safety will be delivered through a variety of approaches, including face to face twilight sessions, inset days and Internet Safety days using both internal and external trainers.

3.2 Learner access to Internet

The internet is an essential element of modern life for education, business and social interaction. St. John's has a duty to provide learners with quality internet access as part of their learning experience. Learner facing staff also have a duty to ensure that they get the balance right between active and passive activities in both education and care time. The internet is used at St. John's to raise educational standards, promote learner achievement and as a necessary tool for staff to support their professional work.

Access to the internet is blocked for learners at certain times of the week to promote more active learning styles for our young people. However, all learners have good access to the internet outside of the blocked times. This policy takes account of the different needs of young people in education and care settings reflecting the difference between being at school or college and being at home. This is kept under review and may change according to circumstances.

- Learners will be taught what internet use is acceptable and what is not. They will be given clear objectives for internet use.

- Learners will be encouraged to tell a staff member immediately if they encounter any material that makes them feel uncomfortable.

- School and college internet access will be filtered for all learners. In some cases, specific learners will be allowed / not allowed to visit certain websites or perform certain keyword searches if this is requested by the learner's tutor (or support worker) and authorised by the Safeguarding team, who then submit the request to IT.

- The school and college will ensure that use of internet derived materials by staff and learners complies with copyright law.
- Processes will be in place for dealing with any unsuitable material found in internet searches.

3.3 Risk Management

St. John's will take all reasonable steps to mitigate the risks associated with internet use and ensure that users create and access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school or college computer.

3.4 Web Content Filtering

St. John's will do all that it can to make sure the network is safe and secure. St. John's will work in partnership with the Internet Service Provider to ensure systems to protect learners are reviewed and improved on a frequent basis. Security software will be up to date.

Appropriate security measures will include the use of enhanced content filtering and protection of firewalls, servers, routers, work stations and so on to prevent accidental or malicious access of systems and information.

If staff or learners discover any unsuitable sites, the URL, content, user who made the discovery, time it was discovered and device that was being used must be reported to the IT Manager.

If the cyber material reported is illegal, St. John's will inform the appropriate authorities as well as notifying internal teams (that is E-Safety, HR and Safeguarding).

3.5 Email

Staff and learners may only use official school and college email accounts on St. John's devices. Governors and Trustees are given St. John's email accounts in order to communicate with St. John's staff and send and receive confidential documents securely.

Learners will be encouraged not to reveal personal details of themselves or others in email communication (such as address or telephone number).

Learners will be guided and supported to immediately tell a staff member if they receive an offensive email.
Personal email addresses must not be used for communication between staff and learners or parent/carers.

3.6 Social Networking

Learners will be given advice on security and privacy settings by staff supporting them, should they wish to access social media during their free time.

Staff should never befriend learners (present or former) on social networking sites.

3.7 Mobile Phones

Where learners have mobile phones, staff must ensure that they are supported to use their devices safely and appropriately.

Learners should refrain from using their mobile phones whilst in lessons. Learners attending St. John's school will be required to hand in personal phones at the start of the day (they will be returned at the end of the day).

Staff should never share their work or personal mobile numbers with learners.

3.8 Emerging Technologies

Emerging technologies will be examined for educational benefits and, where appropriate, risk assessments will be formulated before their introduction. The appropriate use of learning platforms will be determined as technologies become available.

3.9 Acceptable use

The ICT Acceptable Use Agreement for Learners clarifies the expectations and responsibilities of learners when accessing the internet and St. John's devices. This information is also conveyed to parents/carers of learners.

4. Monitoring

Active monitoring of internet data helps ensure that incidents are reported as soon as they occur. Digital communications, including email and internet postings, over the network and over the internet (to the extent possible) will be monitored.

Reports of learner activity can be requested from the IT department. If a learner is specifically vulnerable, regular reports of online activity can be provided to the Safeguarding Team.

5. Policy Enforcement

The IT Manager will ensure that the E-Safety Policy is implemented and that compliance with the policy is monitored.

- The ICT Acceptable Use Agreement for Learners will be referred to in teaching and learning sessions where appropriate and breaches of it will be referred directly to the IT Manager.

- E-Safety rules will be posted in all rooms where computers are used and will be discussed with learners at the start of each academic year.

- Learners will be informed that internet use will be monitored and sanctions will be imposed if the facility is abused.
- If a learner wishes to report an incident they can do so to their tutor, their keyworker, the safeguarding team.
- All staff including teachers, learner support workers/keyworkers, bank, agency staff, will be told how to access this E-Safety Policy and its importance will be explained.

6. Development, Monitoring and Review

This E-Safety policy will be developed, monitored and reviewed by the E-Safety Committee comprising: Designated Safeguarding Leader, Safeguarding Manager, Functional Skills Co-ordinator, Assistive Technology Consultant, representatives from St. John's school and college care teams, IT Manager, Head of HR, Director of Operations and Lead Governor for Safeguarding. The E-Safety Committee will:

- Ensure that the E–Safety policy is regularly reviewed, up to date and that updates are communicated to all users
- Ensure training is delivered in an accessible and timely manner to Governors, staff and learners
- Provide regular reports to the Governing Body
- The E–Safety Committee will audit IDMT provision to establish if the e-safety policy is adequate and that its implementation is effective
- Map and review the e-safety curricular provision ensuring relevance, breadth and monitoring network/internet/incident logs
- Ensure that incidents of misuse are appropriately logged, reported and responded to
- Monitor improvement actions using 360-degree reviews

7. Parental Support

Parents' attention will be drawn to the St. John's E-Safety Policy at enrolment, in newsletters, the St. John's website, during e-safety events and during the annual e-safety week.

E-safety issues will be handled sensitively to inform parents without undue alarm.

A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe IDMT use at home.

Appendix A

Online Safety
DfE Keeping children safe in education (Annex C), September 2018

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 85-87. Resources that could support schools and colleges include:

- UKCCIS (UK Council for Child Internet Safety) has recently published its Education for a connected world framework. Online safety is a whole school and college issue. The framework aims to support the development of the curriculum and is of particular relevance to PSHE education and Computing. It is designed, however, to be usable across the curriculum and beyond and to be central to a whole school or college approach to safeguarding and online safety. It covers early years through to age 18.

- The PSHE Association provides guidance to schools on developing their PSHE curriculum – www.pshe-association.org.uk

- Parent Zone and Google have developed Be Internet Legends a free internet safety curriculum with PSHE accredited lesson plans and teaching resources for Key Stage 2 pupils.

Filters and monitoring

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

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 and 4G 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. UKCCIS have recently published online safety in schools and colleges: Questions for the governing board

Staff training

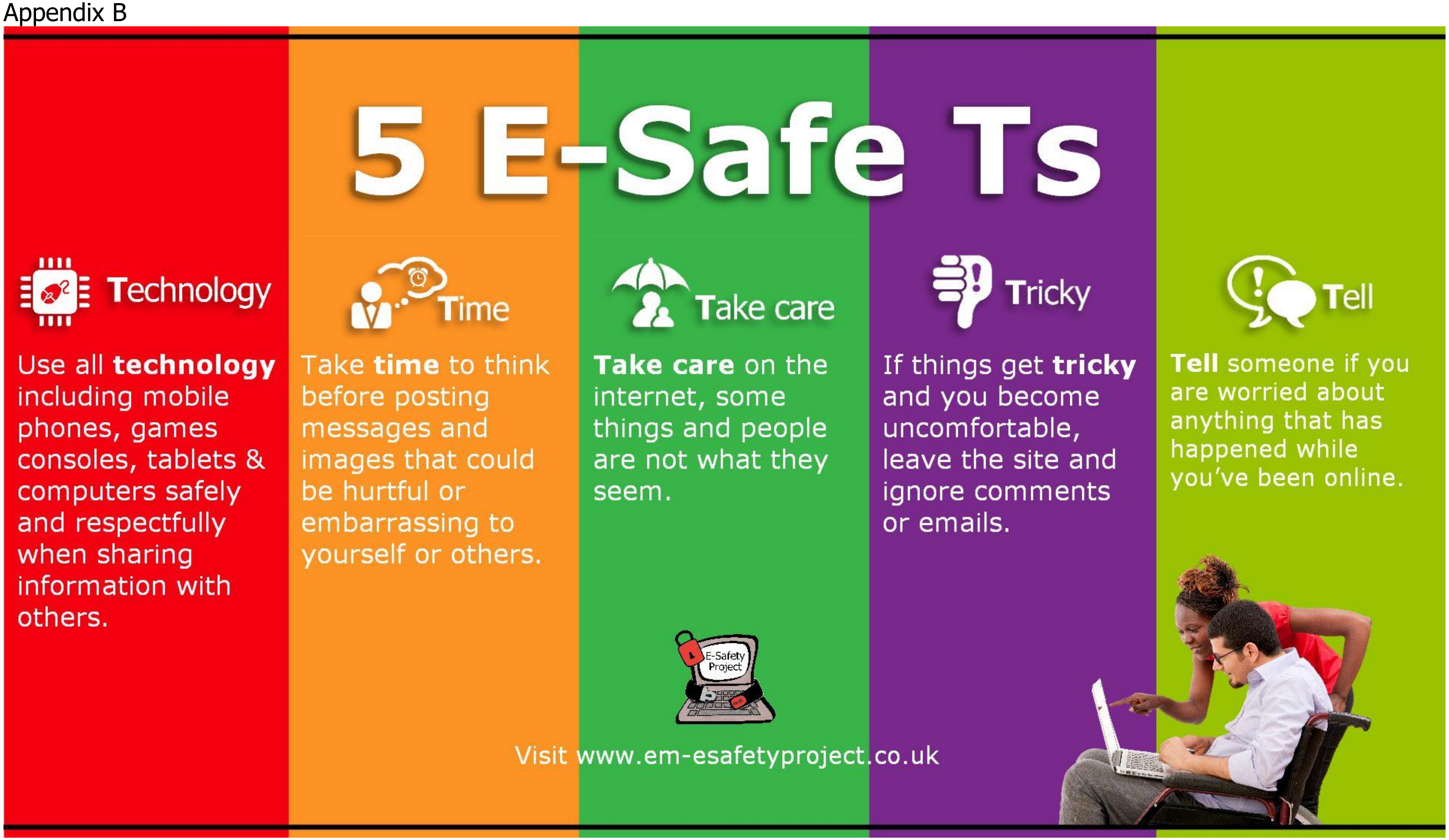
Governors and proprietors should ensure that, as part of the requirement for staff to undergo regularly updated safeguarding training (paragraph 81) and the requirement to ensure children are taught about safeguarding, including online safety (paragraph 85), that online safety training for staff is integrated, 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 to keep children safe online. The following list is not exhaustive but should provide a useful starting point:

Organisation/Resource	**What it does/provides**
thinkuknow	NCA CEOPs advice on online safety
disrespectnobody	Home Office advice on healthy relationships, including sexting and pornography
UK safer internet centre	Contains a specialist helpline for UK schools and colleges
swgfl	Includes a template for setting out online safety policies
internet matters	Help for parents on how to keep their children safe online
parentzone	Help for parents on how to keep their children safe online
childnet cyberbullying	Guidance for schools on cyberbullying
pshe association	Guidance and useful teaching resources covering online safety issues including pornography and the sharing of sexual images
educateagainsthate	Practical advice for parents, teachers and governors on protecting children from extremism and radicalisation.
the 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
UKCCIS	The UK Council for Child Internet Safety's website provides: • Sexting advice • Online safety: Questions for Governing Bodies • Education for a connected world framework
NSPCC	NSPCC advice for schools and colleges
net-aware	NSPCC advice for parents
commonsensemedia	Independent reviews, age ratings, & other information about all types of media for children and their parents
searching screening and confiscation	Guidance to schools on searching children in schools and confiscating items such as mobile phones
lgfl	Advice and resources from the London Grid for Learning
https://www.gov.uk/government/publications/protecting-children-from-radicalisation-the-prevent-duty	The Prevent duty Departmental advice for schools and childcare providers and Prevent Duty Guidance For Further Education Institutions

Appendix B



5 E-Safe Ts

Technology

Use all **technology** including mobile phones, games consoles, tablets & computers safely and respectfully when sharing information with others.

Time

Take **time** to think before posting messages and images that could be hurtful or embarrassing to yourself or others.

Take care

Take care on the internet, some things and people are not what they seem.

Tricky

If things get **tricky** and you become uncomfortable, leave the site and ignore comments or emails.

Tell

Tell someone if you are worried about anything that has happened while you've been online.

Visit www.em-esafetyproject.co.uk