Document name
E-Safety Policy

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

Senior Manager Responsible	
Author	Karen Grist
Superseded Documents	N/A
Date of Latest Review	November 2015
Date of Next Review	November 2017
Associated Documents	Prevent Duty 2015, Data Protection Policy Safeguarding Policy, Whistle Blowing Policy, DfE Guidance for Safer Working Practice for Adults who work with Children and Young People ICT Acceptable User Agreement

Equality Impact Assessment		
Name	Comments	Date
Pam Mason	Approved	Nov 2015

SLT Approval	Approval Date:
✓	02/12/2015
Senior Manager Approval	Approval Date
✓	02/12/2015
Adopted by Governing Body	Adoption Date
✓	01/02/2016

Contents of document

E-Safety Policy

1. Overall Purpose

1.1 The purpose of this policy is to safeguard all learners from the risks associated with the use of digital technologies and to provide a framework to nurture a safe digital community.

1.2 This policy applies to all users, all learners, staff and all members of the school and college community (including volunteers, parents/carers, visitors and community users) who have access to the IT systems, both on the premises and remotely.

1.3 This policy applies to all use of the internet and forms of electronic communication such as email, mobile phones, and social media sites.

1.4 Our approach is to implement appropriate safeguards within St Johns whilst educating and supporting staff and learners in safe use of a range of different digital technologies. We promote and support the development of our learners' ability to identify and manage risks as independently as possible whether at work, school, college or home.

1.5 We aim to achieve this through a combination of security measures, training, guidance, external SWGFL support (Boost) and implementation of our policies.

1.6 This policy should be read in conjunction with the Data Protection and Information Sharing Policy, Safeguarding Policy and Whistle Blowing Policy. There is other legislation and guidance that should also be considered when adhering to this policy.

2. What is E-Safety?

2.1 E-Safety refers to child protection and safeguarding of both children and adults in the digital world. It is about learning to understand and use technologies in a safe, positive way, also about supporting children and adults to develop safe online behaviours (both in and out of the school and college).

2.2 E-Safety is largely concerned with internet communications. The internet is accessible from computers, laptops, tablets, mobile phones, games consoles and other devices like the iPod Touch and internet connected TV. Other communication technologies such as texting and phone calls are also covered by the term 'E-Safety'.

Risks in using the internet include:

- Exposure to inappropriate materials. For example, pornographic pictures and videos.
- Physical danger and sexual abuse. For example, through 'grooming' by paedophiles.
- Cyberbullying – persistent bullying through the digital medium.
- Losing control over pictures and videos.
- Obsessive use of the internet and ICT. For example, addiction to video games.
- Damage to online reputation.
- Inappropriate or illegal behaviour. For example, exposure to hate mail or offensive images, radicalisation, terrorism, illegal downloading, financial scams.
- Viruses, hacking and security.
- Copyright infringement. For example, the illegal sharing of music, pictures, video documents.

3. Use of Internet

3.1 The internet is an essential element of modern life for education, business and social interaction. The school and college have a duty to provide students with quality internet access as part of their learning experience. It 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.

- Learners will be taught what internet use is acceptable and what is not. They will be given clear objectives for internet use.
- Staff will guide learners in online activities that will support the learning outcomes planned for the learners' age and maturity.
- Internet access will be planned to enrich and extend learning activities.
- Learners will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- Learners will be encouraged to tell a staff member immediately if they encounter any material that makes them feel uncomfortable.

- Learners will be taught to question information before accepting it as true.
- School and college internet access will be filtered appropriate to the ability of the learners.

- 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 is found in internet searches.

3.2 Email

- Staff and learners may only use official school and college email accounts on St John's devices.

- All emails sent must be professional in tone and content.

- Personal email accounts must not be used for communication between staff and learners or parent/carers.

- Personal information (as defined in the Personal Data and Information Sharing Policy) must not be emailed to external email addresses from school or college email accounts as emails are sent in an unencrypted format which is not secure.

- Personal information must not be emailed from staff to the official St John's email address and vice versa, as emails are sent in an unencrypted format which is not secure.

- Learners will have been supported through an E Safety awareness session before they use a St John's sanctioned email address.

- Learners will be guided and supported to immediately tell a staff member if they receive an offensive email.

- Learners will be guided in E-Safety awareness sessions about not revealing personal details of themselves or others in email communication (such as address or telephone number). Learners will be guided not arrange to meet anyone without specific permission.

- Emails sent to an external organisation must be written carefully and authorised by managers before sending.

3.3 Social Networking

3.3.1 Staff and learners will behave responsibly and professionally at all times in connection with the use of social networking sites.

Staff will:

- ensure that all communication with learners (including on-line communication) takes place within clear and explicit professional boundaries as set out in the DfE Guidance for Safer Working Practice for Adults who work with Children and Young People and St John's Professional Boundaries Policy.

- raise any concerns to the E-Safety Officer that any colleague(s) is/are not acting in accordance with this policy.

- use their professional judgment and where no specific guidance exists, take the most prudent action possible and consult with the E-Safety Officer if they are unsure.

- cooperate with management in ensuring the implementation of this policy.

- respect the privacy and feelings of others.

- keep a professional distance from learners and ensure a clear separation of the private social lives of workers at the St John's and those of learners.

3.3.2 Use of chatrooms and instant messaging must be in line with the ICT Acceptable User Policy.

3.3.3 Visitors/contributors may be invited to engage through Skype or video conferencing in specific activities such as learner review meetings.

3.4 Mobiles, cameras and portable digital devices

3.4.1 Any use of personal mobile phones, cameras and portable digital devices in school and college by learners and staff must be undertaken in line with the ICT Acceptable Use Policy.

3.5 User Agreement

3.5.1 Staff must not use personal devices to take any images, video or sound recordings of learners.

3.5.2 Staff may take digital photographs and video images to support educational aims but must follow guidance in the ICT Acceptable User Agreement concerning the taking, sharing, distribution and publication of those images using St John's equipment to support education.

3.5.3 Text messaging must not be used for communication between staff and school age learners. For adult learners in the college, or if it is of educational benefit, using St John's owned mobiles.

3.5.4 Staff who are issued with iPads must sign the appropriate agreement.
Memory sticks must be hardware encrypted. This includes portable USB flash drives and portable hard disk drives.

3.5.5 Learners' personal information will not be published. Website photographs that include learners will be selected carefully and will only be published with parental or learner (dependant on age and mental capacity) permission.

3.5.6 Learners' full names will not be used anywhere on the website, particularly in association with photographs.

3.5.7 The CEO/Principal will delegate editorial responsibility to the IT Manager to ensure that content is accurate and quality is maintained.

3.6 Cyberbullying

3.6.1 Cyberbullying is the use of the internet and related technologies to harm other people, in a deliberate, repeated and hostile manner. When young people are the target of bullying via mobile phones, gaming or the internet, they can often feel very alone and a previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety.

Learners will be:

- taught about the effects of cyberbullying
- encouraged to keep any evidence of cyberbullying
- made aware that the police will be able to trace the originator of any messages

3.6.2 Cyberbullying (along with all forms of bullying) will not be tolerated in the school or college. All incidents reported will be recorded and investigated.

4. Filtering

4.1 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. Security software will be up to date.

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

4.3 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.

4.4 If the cyber material reported is illegal, St johns will inform the appropriate authorities as well as notifying internal teams; E-Safety/HR/Safeguarding Team.

5. Monitoring

5.1 Active monitoring of internet data will 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.

5.2 The IT department will provide monthly reports of learner online activity to the Safeguarding Team.

6. Policy Enforcement

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

6.2 The ICT Acceptable User Agreement for Learners will be referred to in teaching and learning sessions where appropriate and breaches of it will be referred directly to the E-Safety Coordinator.

6.3 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.

6.4 Learners will be informed that internet use will be monitored and sanctions will be imposed if the facility is abused.

6.5 Learners will be informed that network and internet use will be monitored.

6.6 If a learner wishes to report an incident they can do so to their tutor, their keyworker, the safeguarding team or via SWGFL 'Whisper' anonymous reporting tool.

6.7 All staff must read and sign the ICT Acceptable User Agreement before using school and college ICT resources and annually thereafter.

6.8 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.

6.9 Staff will be made aware that professional conduct is essential when using school and college ICT and that internet use will be monitored and can be traced to the individual user.

6.10 Any breaches of the ICT Acceptable User Agreement for staff will be referred directly to the E-Safety Coordinator.

6.11 St John's will keep a record of all staff that have been denied internet access and the reason and length of time it was denied.

7. Parental Support

7.1 Parents' attention will be drawn to the school E-Safety Policy in newsletters, the school website, during e-safety events and during the annual e-safety week.

7.2 Internet issues will be handled sensitively to inform parents without undue alarm.

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

8. Education and Training

8.1 Training in E-safety will be delivered through a variety of approaches, including e-training and face to face twilight sessions, inset days and Internet Safety days using both internal and external trainers. The training will be based on BOOST Plus E-safety training package and will be delivered at staff induction and annual scheduled intervals.

9. Risk Management

9.1 St Johns will take all reasonable steps to mitigate the risks identified above 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.

9.2 An E-Safety Coordinator has been appointed and will work with the IT Manager to oversee internet dangers, risk assessment and matters arising from internet use.

10. Development, Monitoring and Review

10.1 This E-Safety policy will developed, monitored and reviewed by the E-Safety Committee comprised of; E-Safety Officer, Vice Principal, Senior Safeguarding Lead, Lead Governor for Safeguarding, Head of HR, SWGFL E-Safety Advisor

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 ICT 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
- Implementation of the e-Safety rules will be checked regularly by the E-Safety Coordinator
- Ensure that incidents of misuse are appropriately logged, reported and responded to
- Monitor improvement actions through the use of the 360 degree reviews