Staff Internet and ICT Acceptable Use Policy (AUP) & E-Safety Policy

Reviewed and Approved by the Personal, Development, Behaviour and Welfare Committee
On: 12 October 2017

Reviewed and Ratified at the St Edward's FGB date
On: 14 December 2017

Next review date: December 2020

Member of SLT responsible: Mr A Bousfield

Discretionary Rights
St Edward's School reserves the right to vary the terms of this policy at any time and without prior notice. Staff will be informed of any such changes. St Edward's School has the right to withdraw access to the Network and/or other services. The decision of St Edward's School is final.

Forward:-
St Edward's School has a responsibility to clarify acceptable use of the ICT facilities including internet use for all Staff to ensure the ICT facilities are used in a responsible and professional manner. As part of the policy all stakeholders are expected to be familiar with, and comply with, all aspects of the AU Policy.

The law requires each school to monitor the use of the school's computer systems, including access to web-sites, the interception of email and the deletion of inappropriate materials. This includes a periodical check on anything that is on the school's equipment and all items are considered the property of the school.

All Staff must be aware that the School Internet Provider and the School's Network Manager/ICT Technical Coordinator is required to proactively monitor the use of the system. In the case of the Internet provider, major criminal abuse is reported directly to the Police and not to the school. The Internet provider and the Police may prosecute the person whose username has been used and saying that it was used by a third party it will be no defence – this is a Government policy. Please contact the school's Network Manager/IT Strategy Lead if further clarification is required.

Staff must also be aware of what to do if they find or suspect criminal and inappropriate use by another member of staff. Staff have a legal duty to preserve any evidence of criminal activities, failure to do so may also be a criminal activity. Staff are directed to the school's Whistleblowing policy.

St Edward's Acceptable Use Policy
This policy forms the basis of an 'acceptable use' agreement form that all staff are required to sign. Breaches of the agreement will be passed to the Headteacher. This policy stands *in addition* to the Internet provider policy and the Esafety Policy which is contained herein. Staff who use the school systems will be considered to have accepted this policy and any future amendments which will be stored on the 'Staff Only' drive (Q) Policies section.

Educational Purpose
The St Edward's School Network has been established for an educational purpose. The term "educational purpose" includes classroom activities, career development, and quality educational research activities using the internet.

Designated Person
Staff are required to know who the 'Designated Person for Safeguarding' is within the school (See the Child Protection and Safeguarding Policy). Acceptable use concerns and issues regarding the ICT facilities should be reported to the Network Manager or the Deputy Head as appropriate.

Staff Internet and email access

1. Personal Use. You may use the school network for personal purposes as long as it does not breach this policy and is kept within professional boundaries. For example spending many hours pursuing personal interests that are not part of continuous professional development or educational are not considered professional.
2. Inappropriate Access to Material.
    a. You may not use The St Edward's School Network to access internet material that is inappropriate or offensive. The Headteacher holds the right to decide what the school considers to be inappropriate and offensive.
    b. If you mistakenly access inappropriate material on the internet, you should immediately tell the Network Manager/ICT Technical Coordinator who may also need to inform the Headteacher. This may protect you against a claim that you have intentionally violated this Policy.

3. You may use web-based Email for school and personal use. The school reserves the right to block any e-mail services that they consider to be unsafe or inappropriate. All emails sent and received are considered the responsibility of the user. You may not send emails which could cause offence to others. You may not access emails in school which contain material that could be considered inappropriate or offensive, therefore if you have any doubts about emails sent to you do not access them. Staff should only communicate with students through the school email system or other school Office 365 systems.

4. Staff have access to some websites not accessible by students, e.g. "Youtube". It is important that staff do not allow any student access to these resources via any staff logon as this would be a major breach of this policy, also this increased staff access is for educational purposes only.

Use

The following points should be noted when using the St Edward's School ICT facilities:

1. **Personal Safety:**
   a. You should be aware of the dangers of entering personal information into webpages or emails.

   b. You should immediately tell the Network Manager/IT Strategy Lead if you receive inappropriate material via a web interface or email system.

   c. You may not use any chatroom or messaging system that has not been authorised (including communicating with students).

   d. You may not publish school related information onto personal web sites without approval from the Headteacher.

   e. You may not develop or edit personal websites at school.

   f. Communicating with students via Facebook or other social network is considered to be inappropriate and puts both parties at risk. Staff have a responsibility to stop this from happening and secure their profile from access by students.

2. **Activities:**
   a. You may not attempt to gain unauthorised access to the St Edward's School Network or go beyond your authorised access. This includes attempting to log-on through another staff member's account or access another staff member's files.

   b. You should not make deliberate attempts to disrupt the computer systems.

   c. You should not pass confidential school data or files to third parties without consent.

   d. If authorised data is required to be passed to third parties you must ensure that the data is secure and not sent via insecure email or similar methods.

   e. You should not intentionally introduce computer virus or malware on to the school network system.

   f. Digital images of students may not be posted to any website, chatroom or passed to any person outside school without authorisation.

   g. Staff may not post images of any school activity, student or school premises (including trips, sports events, camps or school social activity) to any website, social network

(including Facebook and twitter) or any open access system. Staff may not use **personal** imaging devices (cameras, mobile phones, etc) to take any of these images.

h. You are not allowed to download, or copy to the network, any music, video and other materials which is copyrighted unless the school holds the permission of the copyright holder.

i. You may not use the St Edward's School Internet access for any business purpose including buying or selling. This includes development of websites for other parties.

j. Due consideration must be given to the cost of large printouts and whether there are more economic alternatives.

k. You may not allow a student access to the network via your username and password as there are many confidential files that they would have access to and you would be in breach of the Data Protection Act and fines of up to £500,000 apply to you.

l. You should maintain the security of the system at all times. This includes never leaving a machine logged in where a student may gain access.

m. You may not allow siblings to use your username & password or laptop.

n. You should not allow visitors access through your logon. This is to maintain security and confidentiality.

o. All school staff should also adhere to a professional level of conduct in their own internet use outside of school as well as within.

p. In their private use of digital media (such as social networking sites or other digital communication systems) staff must protect their professional reputation, the reputation of the school and staff in partner organisations. This must be achieved either through the judicious application of privacy settings so that communications/images/etc. remain private from children and young people / parents and carers and through the avoidance of rhetoric that might cause reputational damage. Staff must also make sure that none of their digital activities could bring the school into disrepute in any form whatsoever.

q. Staff should also encourage students to use the ICT facilities and the internet responsibly, at home or at school, whenever it is appropriate. This is important especially during lessons.

r. Staff are required to ensure that students in years 7 to 11 are fully and actively monitored during their use of any school computer equipment and to take steps when they find students breaking this rule. There needs to be partial supervision for Sixth Form.

s. Staff are expected to inform the school's Network Manager and/or the Headteacher if they believe that others are not following these rules.

t. Staff should not normally download or store school data or files on any equipment that does not belong to the school. Where it is absolutely necessary and authorised you must ensure that no other user of that computer or equipment can access the data or files and the data or files are deleted as soon as possible. This includes the MIS data.

3. **System Security:**
   a. You are responsible for your individual user area and should take all reasonable precautions to prevent others from being able to use it. **You should not let any other person know your password.** Staff who allow students access via a staff logon (even if only briefly or monitored) will be considered to have allowed a major breach of system security and disciplinary procedures may be brought against the member of staff by the Headteacher. Leaving a computer in an insecure state (logged in but not locked in an insecure area) may also result in disciplinary procedures by the Headteacher.

   b. You should immediately notify the IT Strategy Lead or the Network Manager if you have identified a possible security problem. Do not go looking for security problems because this may be construed as an illegal attempt to gain access.

   c. You may not download computer programs or games from the Internet.

   d. You may not try to load computer programs or games onto the St Edward's School Network or attempt to run programs that are not accessed through the normal menu structure.

   e. Access to the school network from an external source (the internet) must only be from a secure, safe computer that has current, up to date, virus protection. The use of internet cafes or public-access places are not considered safe and must not be used.

   f. When you have finished using the school systems from an external computer you must close ALL browser windows to maintain security.

4. **Email misuse:**
   a. You should not email information that could cause damage or a danger of disruption.

   b. You should not use the ICT facilities to bully another person. You should not email private information about another person.

   c. You should not email chain letters or engage in "spamming".

   d. All email use should be kept professional in tone and content.

5. **Misuse of resources**:
   a. Please avoid unnecessary printing. Printers may only be used for school purposes.

   b. Accessing and playing games, on-line gambling etc. via the Internet is not allowed.

   c. You should not misuse or neglect any equipment in such a way so that it is likely to damage or destroy any school property.

   d. You will not remove any ICT equipment from its position without the express permission from the Network Manager or from the SLT.

6. **Data Protection:**

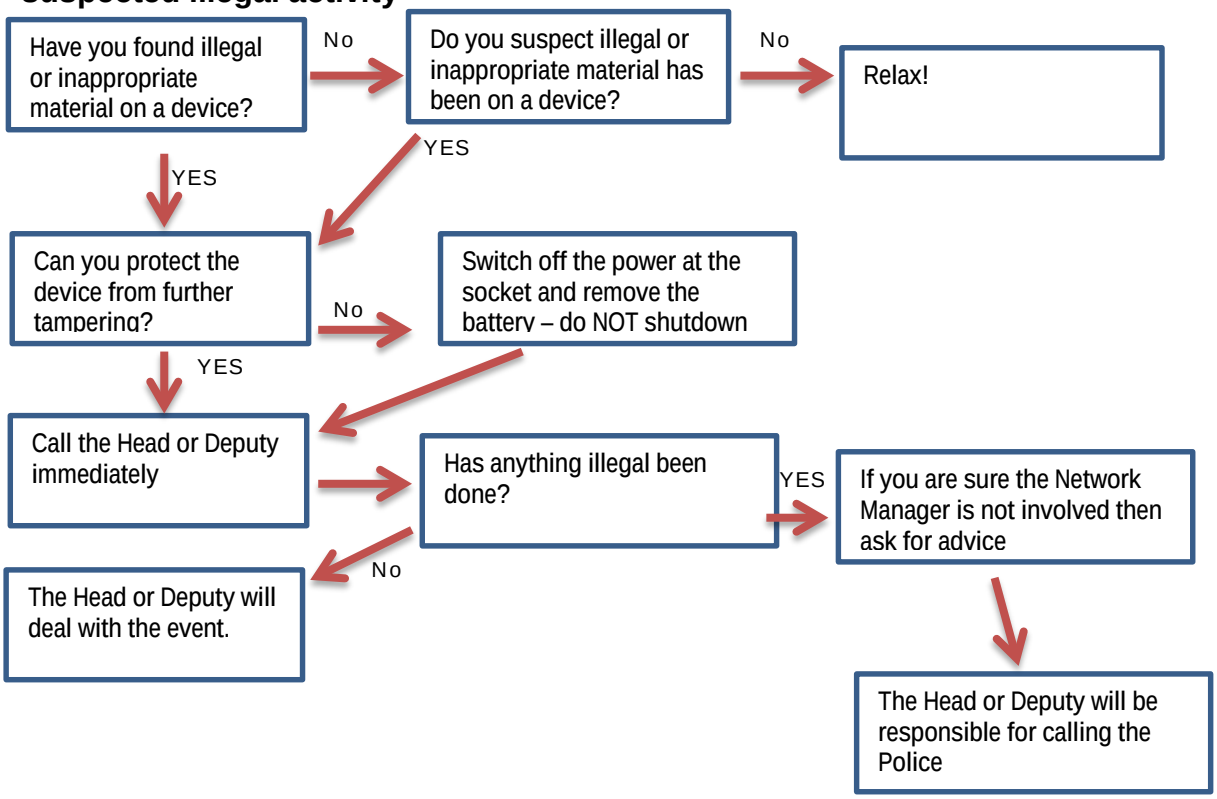
   a. **Staff must follow strict data protection guidelines in that all data is considered confidential and must not be passed onto other parties within the school who do not have access to that data, it must not be passed onto third parties without permission from the Headteacher and must not be used for any personal**

purpose whatsoever as this would put you in breach of data protection laws.

b. Staff have a duty of care to ensure that any laptop, memory stick or other storage device does not fall into the hands of others. The Information Commissioner's Office (www.ico.gov.uk) can now issue monetary penalty notices of up to £500,000 where breaches occur. They are able to fine both the school and the individual concerned.

c. Any incident must be reported to our Business and Premises Manager who is also our Data Protection Officer.

7. **Emergency procedure for ALL staff in the event of finding someone engaged in suspected illegal activity**



8. **Creating, publishing, distributing & receiving illegal material**
It is important that you understand the law on illegal material. Failure to do so could render you or others liable for prosecution. The best way to understand this is to give some examples to show who has broken the law.

I. A student takes an illegal image of another student (The student has **created** illegal material)
II. The student shows their friends the image (the student has **published** this material)
III. The student sends the image to others (the student has **distributed** the material and everyone has **received** illegal material)
IV. A member of staff sees/becomes aware of the image (nothing)
V. The member of staff asked the student to save/send/copy the image elsewhere (**both** the member of staff and the student has broken the law – **creating, publishing, distributing and receiving** illegal material.
VI. The member of staff checks the image a couple of times (**receiving**)
VII. The member of staff shows the image to another member of staff (**publishing and receiving**)

VIII. The member of staff passes the image on to another person (**distributing** and **receiving**)

Each person here has **intentionally broken the law** and could face prosecution. Your reputation could be damaged – especially if the newspapers published a headline "Mr XXX of St Edward's School has been suspected of 'receiving child pornography' ". If in doubt contact the Designated Safeguarding Lead as soon as possible.

9. **Staff responsibility for students at St Edward's**
Due to the changes in law all staff at St Edward's MUST have due regard of the PREVENT duty.

The following is an excerpt from Safeguarding KCSIE_Part_1_July_2015.pdf document. For further information and assistance seek help from the designated person for safeguarding at St Edward's.

From 1 July 2015 specified authorities, including all schools as defined in the summary of this guidance, are subject to a duty under section 26 of the Counter-Terrorism and Security Act 2015 ("the CTSA 2015"), in the exercise of their functions, to have "due regard[12] to the need to prevent people from being drawn into terrorism"[13] This duty is known as the Prevent duty. It applies to a wide range of public-facing bodies. Bodies to which the duty applies **must have regard to statutory guidance issued under section 29 of the CTSA 2015** ("the Prevent guidance"). Paragraphs 57-76 of the Prevent guidance are concerned specifically with schools (but also cover childcare).

The statutory Prevent guidance summarises the requirements on schools in terms of four general themes: risk assessment, working in partnership, staff training and IT policies.

• Schools are expected to assess the risk of children being drawn into terrorism, including support for extremist ideas that are part of terrorist ideology. This means being able to demonstrate both a general understanding of the risks affecting children and young people in the area and a specific understanding of how to identify individual children who may be at risk of radicalisation and what to do to support them. Schools and colleges should have clear procedures in place for protecting children at risk of radicalisation. These procedures may be set out in existing safeguarding policies. It is not necessary for schools and colleges to have distinct policies on implementing the Prevent duty.

• The Prevent duty builds on existing local partnership arrangements. For example, governing bodies and proprietors of all schools should ensure that their safeguarding arrangements take into account the policies and procedures of Local Safeguarding Children Boards (LSCBs).

• The Prevent guidance refers to the importance of Prevent awareness training to equip staff to identify children at risk of being drawn into terrorism and to challenge extremist ideas. Individual schools are best placed to assess the training needs of staff in the light of their assessment of the risk to pupils at the school of being drawn into terrorism. As a minimum, however, schools should ensure that the designated safeguarding lead undertakes Prevent awareness training and is able to provide advice and support to other members of staff on protecting children from the risk of radicalisation.
• Schools must ensure that children are safe from terrorist and extremist material when accessing the internet in schools. Schools should ensure that suitable filtering is in place. It is also important that schools teach pupils about online safety more generally.

The Department for Education has also published advice for schools on the Prevent duty. The advice is intended to complement the Prevent guidance and signposts other sources of advice and support.

[12] According to the Prevent duty guidance 'having due regard' means that the authorities should place an appropriate amount of weight on the need to prevent people being drawn into terrorism when they consider all the other factors relevant to how they carry out their usual functions.

[13] "Terrorism" for these purposes has the same meaning as for the Terrorism Act 2000 (section 1(1) to (4) of that Act).

Supporting information

http://ceop.police.uk/ For advice and guidance from the Police's Child Exploitation and Online Protection Unit (CEOP)

http://www.swgfl.org.uk/Staying-Safe For e-safety support material from the South West Grid for Learning who provide Internet connectivity to nearly all state schools in the 15 South West local authorities as well as actively managed filtering and monitoring. This includes Standard Acceptable User Policies, bring your own device, advice on clouding etc.

http://www.iwf.org.uk/ Internet Watch Foundation ,for the reporting of criminal online content.

http://www.e2bn.org/files/Inspecting_e-safety.pdf Inspecting e-safety Ofsted 2012

https://www.gov.uk/data-protection/the-data-protection-act Data Protection Act 1998

http://www.ofsted.gov.uk/resources/safe-use-of-new-technologies Safe use of new technologies Ofsted 2009

www.education.gov.uk/ukccis Advice on Child Internet Safety 1.0 UK Council for Child Internet Safety

http://www.nspcc.org.uk/Inform/research/briefings/Photographing-children_wda96007.html NSPCC guidance on photos in schools

http://www.ico.org.uk/ Data Protection/Information Commissioner's Office (ICO)

Safe Schools and Communities team ssct@dorset.pnn.police.uk 01202 222844 . This team provides support if an E safety incident occurs as well as training packages for children, young people, parents/carers and staff.

E-SAFETY POLICY

Reviewed and Approved by the Personal, Development, Behaviour and Welfare Committee
On:

Reviewed and Ratified at the St Edward's FGB date
On:

Next review date: December 2020

Member of SLT responsible: Mr A Bousfield

Scope of the Policy

This policy applies to all members of St Edward's community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of St Edward's.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off St Edward's site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of St Edward's but is linked to membership of St Edward's. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data).

St Edwards will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school. St Edward's School expects parents and carers to be aware of, and regulate, their child's online activity.

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within St Edward's;

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor combined with the role of Safeguarding Governor. The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Co-ordinator
- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors / committee / meeting

Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of St Edward's community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator
- The Headteacher and other members of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- The Headteacher / Senior Leaders are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher / 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 e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the E-Safety Co-ordinator

E-Safety Coordinator:

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing St Edward's e-safety policies
- 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 training and advice for staff
- liaises with the Local Authority
- liaises with school technical staff

- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments

Network Manager:

- that St Edward's technical infrastructure is secure and is not open to misuse or malicious attack
- that St Edward's meets required e-safety technical requirements and any Local Authority / other relevant body E-Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering of the network, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- 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 relevant
- that the use of the network / internet / Virtual Learning Environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher or Senior Leader/ E-Safety Coordinator for investigation and action
- that monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff:

are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the Staff ICT Acceptable Use (AUP) and the DFE "Keeping Children Safe in Education" directive.
- they report any suspected misuse or problem to the Headteacher / Senior Leader / E-Safety Coordinator / Officer for investigation and action
- all digital communications with students / parents / carers should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other activities
- students understand and follow the e-safety and acceptable use policies
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students 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 internet searches

Safeguarding Designated Lead:

will be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding 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

Students:

- are responsible for using St Edward's digital technology systems in accordance with the Student Acceptable Use Policy
- 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 policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying and the seriousness of consequences if they are found to be in breach.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that St Edwards' E-Safety Policy covers their actions out of school, if related to their membership of St Edward's

Parents and Carers:

Parents and Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. St Edward's will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters and website. Parents and Carers will be encouraged to support St Edward's in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website and on-line student records
- their children's personal devices in St Edward's
- the monitoring and regulation of their child's online activity, especially that their child's use of social media is responsible and age-appropriate.

Policy Statements

Education – 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 St Edward's e-safety provision. Children and young people need the help and support of St Edward's to recognise and avoid e-safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited and updated in line with new developments i.e. Prevent.
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Students should be 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.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students should be helped to understand the need for the student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that students 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 internet searches.
- Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff need to be aware of these searches and record this in case of future investigation.
- Students should be educated in the potential risk of content related to extremist behaviour or with an agenda to radicalise students. Students taught in line with recommendation from governments Prevent Agenda.

Education – Parents and Carers

Many parents and carers have only a limited understanding of e-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

behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

St Edward's will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, website
- Parents and Carers evenings
- High profile events / campaigns eg Safer Internet Day
- Reference to the relevant websites / publications e.g: https://www.saferinternet.org.uk/

Education & Training – Staff

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

- A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the appraisal.
- **All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand St Edward's e-safety policy and Acceptable Use Agreements.**
- The E-Safety Coordinator / Officer (or other nominated person) 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 in staff / team meetings / INSET days.
- The E-Safety Coordinator (or other nominated person) will provide advice / guidance / training to individuals as required.

Training – Governors

Governors / Directors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub committee / group involved in technology / e-safety / health and safety / 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 organisation (eg SWGfL).
- Participation in school training / information sessions for staff or parents.
- Through Governor monitoring visits

Technical – infrastructure / equipment, filtering and monitoring

St Edward's will be responsible for ensuring that St Edward's infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School technical systems will be managed in ways that ensure that St Edward's meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by the Network Manager who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password
- The "administrator" passwords for St Edward's ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in the school safe.
- The Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list.

- Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes
- St Edward's has provided differentiated user-level filtering which allows different filtering levels for different categories of person i.e. student, staff and SLT etc.
- St Edward's technical staff regularly monitor and record the activity of users on St Edward's technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of St Edward's systems and data. These are tested regularly. St Edward's infrastructure and individual workstations are protected by up to date virus software.
- There is limited provision for guests i.e supply teachers, to have access to the network under the direction of the Network Manager.
- An agreed policy is in place (Staff AUP) regarding the extent of personal use that users and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place (Staff AUP) that forbids staff from downloading executable files and installing programmes on school devices.
- An agreed policy is in place (Staff AUP) regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off St Edward's site unless safely encrypted or otherwise secured.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. St Edward's will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites**.**
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on **school equipment**, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or St Edward's into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Students full names will not be used anywhere on a website or blog, particularly in association with photographs unless parental permission has been given.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on St Edward's website as covered in the AUA signed by parents or carers at the start of the year
- Student's work can only be published with the permission of the student and parents or carers.
  Students are forbidden from taking photos / videos on their own devices at anytime on school site.
- Students are forbidden from posting photos or videos on social media that brings the school into disrepute or for the use of bullying others.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 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 sufficient protection to minimise risk

St Edward's must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".

- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed / identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

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.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how St Edward's currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults			Students			
Communication Technologies	Allowed	Not Allowed	Allowed for selected staff	Allowed	Not Allowed	Allowed at certain times	Allowed with staff permission
Mobile phones may be brought to school	X			X			
Use of mobile phones in lessons		X			X		
Use of mobile phones in social time	X				X		
Taking photos on mobile phones / cameras		X			X		
Use of other mobile devices eg tablets, gaming devices			X				X
Use of personal email addresses in school, or on school network	X			X			
Use of school email for personal emails	X			X			
Use of messaging apps	X				X		
Use of social media		X			X		
Use of blogs	X						X

When using communication technologies St Edward's considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only St Edward's email service to communicate with others when in school, or on school systems (eg by remote access).
- Users must immediately report, to the nominated person – in accordance with St Edward's policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students or parents / carers (email, chat, etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Students should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on St Edward's website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

All schools and local authorities have a duty of care to provide a safe learning environment for students and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render St Edward's or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

St Edward's provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and St Edward's through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made in social media to students parents and carers or school staff
- They do not engage in online discussion on personal matters relating to members of St Edward's community
- Personal opinions should not be attributed to St Edward's or Local Authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

St Edward's uses social media for professional purposes, this must be checked regularly by the SLT and e-safety coordinator to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Unsuitable / inappropriate activities

St Edward's believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. St Edward's policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Extremist material or material that promotes the radicalisation of others or terrorism; (in line with guidance from Government Prevent Agenda.					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of St Edward's or brings St Edward's into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by St Edward's / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational)			X			
On-line gaming (non educational)					X	
On-line gambling					X	
On-line shopping / commerce				X		
File sharing				X		
Use of social media				X		
Use of messaging apps				X		

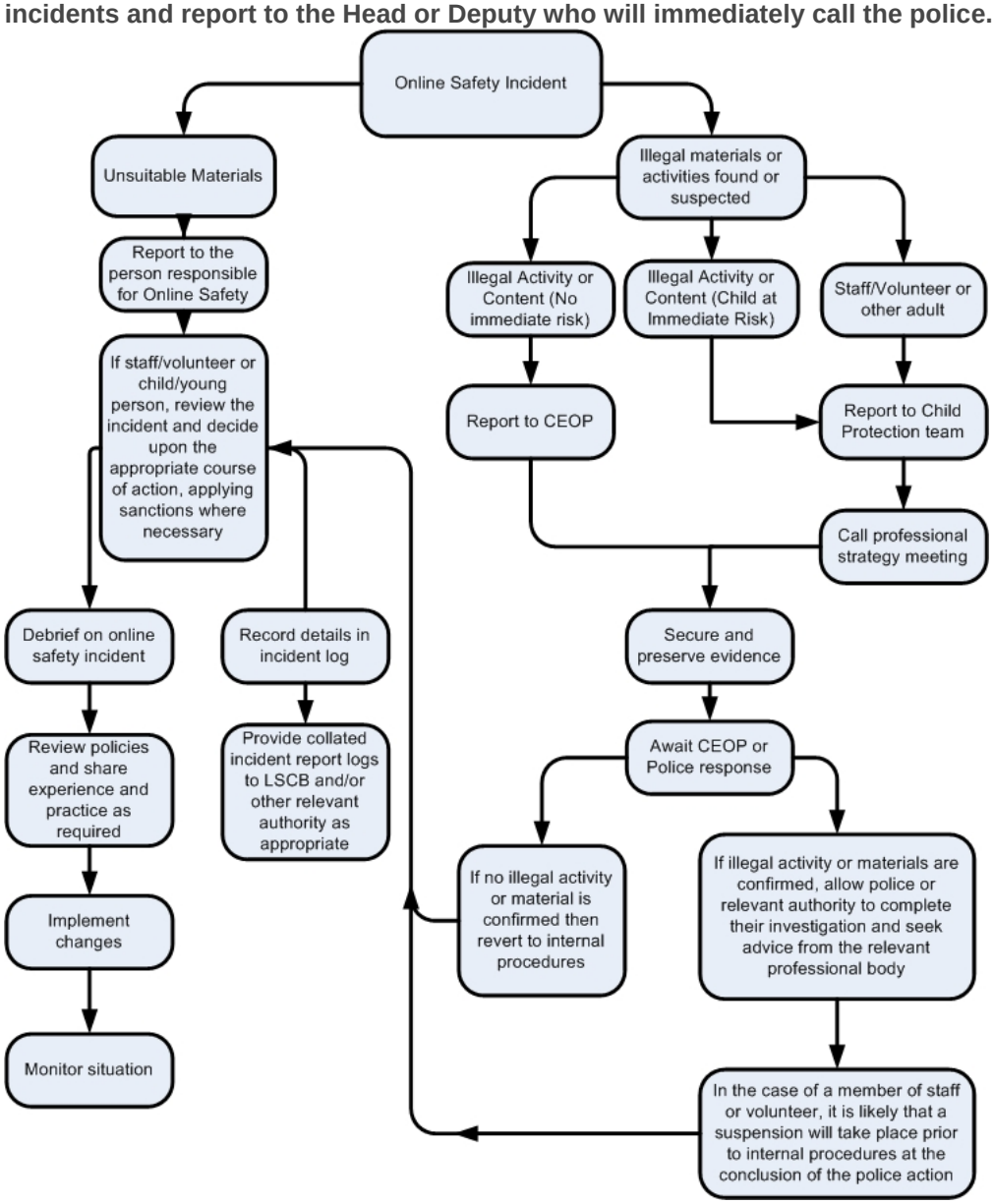
Use of video broadcasting eg Youtube			X		

Responding to incidents of misuse – School procedure

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below) for responding to online safety incidents and report to the Head or Deputy who will immediately call the police.



Other Incidents

It is hoped that all members of St Edward's community will be responsible users of digital technologies, who understand and follow school 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:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to 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 organisation (as relevant).
  - Police involvement and/or action
- If content being reviewed includes images of Child abuse then the monitoring should be halted and 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
  - adult material which potentially breaches the Obscene Publications Act
  - criminally racist material
  - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change 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 St Edward's and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

St Edward's Actions & Sanctions

It is more likely that St Edward's 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 a proportionate manner, and that relevant members of St Edward's community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Students / Pupils — Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Headteacher	Refer to Police (Head or Deputy)	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X					
Unauthorised use of non-educational sites during lessons	X						X		X
Unauthorised use of mobile phone / digital camera / other mobile device	X					X			X
Unauthorised use of social media / messaging apps / personal email	X					X	X		X
Unauthorised downloading or uploading of files	X				X	X	X		X

Allowing others to access school network by sharing username and passwords	X					X	X		X
Attempting to access or accessing St Edward's network, using another student's account	X						X		X
Attempting to access or accessing St Edward's network, using the account of a member of staff		X	X			X	X		X
Corrupting or destroying the data of other users		X			X	X	X		X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X				X	X		X
Continued infringements of the above, following previous warnings or sanctions			X			X	X		X
Actions which could bring St Edward's into disrepute or breach the integrity of the ethos of St Edward's			X			X	X		X
Using proxy sites or other means to subvert St Edward's' filtering system		X				X	X		X
Accidentally accessing offensive or pornographic material and failing to report the incident	X								X
Deliberately accessing or trying to access offensive or pornographic material		X				X	X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			X			X	X		X

The sanctions imposed by the school are at the discretion of the school, and are part of the school's overall right to manage the behaviour of its staff and students both on site and, in certain circumstances, offsite.

Staff Actions / Sanctions

Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Informal Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X			X	X
Inappropriate personal use of the internet / social media / personal email	X	X				X		
Unauthorised downloading or uploading of files	X				X	X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing St Edward's network, using another person's account	X	X			X			X
Careless use of personal data eg holding or transferring data in an insecure manner	X					X		
Deliberate actions to breach data protection or network security rules		X	X		X			X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X		X			X

Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X					X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X	X						X
Actions which could compromise the staff member's professional standing		X						X
Actions which could bring St Edward's into disrepute or breach the integrity of the ethos of St Edward's		X						X
Using proxy sites or other means to subvert St Edward's' filtering system	X					X		
Accidentally accessing offensive or pornographic material and failing to report the incident	X					X		
Deliberately accessing or trying to access offensive or pornographic material		X						X
Breaching copyright or licensing regulations	X				X			X
Continued infringements of the above, following previous warnings or sanctions		X			X			X

Document Links;

- St Edward's Safeguarding Policy
- St Edward's Behaviour Policy
- St Edward's Prevent Policy
- St Edward's Acceptable Use Policy.

Acknowledgements

St Edward's would like to acknowledge a range of individuals and organisations whose policies, documents, advice and guidance have contributed to the development of this E-Safety Policy

- Members of the SWGfL E-Safety Group
- Avon and Somerset Police
- Prevent Strategy (2011)
- DFE Keeping young people safe.