St Peter's School E-Safety Policy

UNCRC Article 3: Everyone who works with children should do what is best for each child.
UNCRC Article 19: Children should not be harmed and should be looked after and kept safe.
UNCRC Article 36: Children should be protected from doing things that could harm them.

Rationale St Peter's School understands both the benefits and risks that modern technology can pose to our community and understands the fact that it is constantly evolving. The school will deal with e-safety incidents in line with 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.

This policy ensures we have rigorous procedures in place to ensure the safety of our pupils, staff and wider community as well as educating our pupils to become confident and resilient users of technology.

This policy applies to all members of the St Peter's School (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 the school.

Roles and Responsibilities Headteacher and Senior Leader

- Have a duty of care for insuring the e-safety of members of the school community
- Are aware of the procedures to be followed in the event of a serious e-safety allegation being made
- Ensure that the E-safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and train other colleagues as relevant

E-Safety Coordinator

- Takes day-to-day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies and documents
- 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 ESC
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.

Technical Staff/Coordinator for ICT & Computing

- Ensure that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- Ensure that the school meets required e-safety technical requirements and any ESC / other relevant body E-Safety Policy / Guidance that may apply.
- Ensure any reports of misuse are passed on to the e-safety coordinator and headteacher.

Teaching and Support Staff

- Report any suspected misuse or problem to the headteacher or deputy headteacher for investigation 2 All digital communications with pupils and 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
- Pupils understand and follow the e-safety and acceptable use policies
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- 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

Child Protection/Safeguarding Designated Person

- 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 o potential incidents of radicalisation

Pupils

- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Are responsible for using the school's digital technology systems in accordance with the Pupil Acceptable Use Policy
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

Parents/Carers

- Encouraged to support the school in promoting good e-safety practice both at home and at school, especially regarding:
- Digital and video images taken at school events
- Their children's personal devices in the school (where appropriate)

Teaching and Learning

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school 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.

We are committed to the following:

- The schools' Internet access includes filtering appropriate to the age of pupils.
- Pupils should be helped to understand the need for the Pupil Acceptable Use Policy and encouraged to adopt safe and responsible use both within and outside school Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the pupils visit.
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- To promote learners' independence and sense of personal responsibility, all pupils will be aware of the Acceptable Use Policy which is displayed in each classroom and in key areas in the school building
- A record is kept of any cyberbullying or inappropriate behaviour in-line with the school's behaviour management system. Parents/carers are informed of significant or repeated inappropriate behaviours.
- The school provides advice and information on reporting offensive materials, abuse/ bullying etc and makes this available for pupils, staff and parents as appropriate.
- E-Safety advice for pupils, staff and parents is provided through:
- Curriculum activities
- Letters, newsletters, website
- High profile events (eg Internet Safety Day)
- Parents/Carers sessions
- Pupils should be taught in all lessons to be critically aware of the materials and content they access online
- The school ensures staff know how to send or receive sensitive and personal data and understand the requirement to protect data through password protection or encryption.
- The E-safety coordinator will receive training to allow him/her to provide updates to the rest of the school community

Pupils will be taught a range of skills and behaviours appropriate to their age and experience, such as:

- To discriminate between fact, fiction and opinion;
- To understand 'Netiquette' behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
- To understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
- To understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
- To understand why they must not post pictures or videos of others without their permission;
- To have strategies for dealing with receipt of inappropriate materials;
- To understand why and how some people will 'groom' others with inappropriate or illegal motives (older pupils)

Bring Your Own Devices

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom of choice and usability. Use of BYOD should not introduce vulnerabilities into existing secure environments.

- The school has a set of clear expectations and responsibilities for all users
- The school adheres to the Data Protection Act principles
- All users are aware of the Acceptable Use Agreement
- All network systems are secure and access for users is differentiated
- Where possible these devices will be covered by the school's normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe

Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils 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. The school 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 pupils 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 ESC, 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/pupils 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 / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

• Written permission from parents or carers will be obtained before photographs of students/pupils are published on the school website

Data Protection Personal data will be recorded, processed, transferred and made available according to the Jersey Data Protection guidelines which states that personal data must be:

• Fairly and lawfully processed 5
• Processed for limited purposes
• Adequate, relevant and not excessive
• Accurate • Kept no longer than is necessary
• Processed in accordance with the data subject's rights
• Secure
• Only transferred to others with adequate protection.

The school 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 Jersey Data Protection Regulations
• 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.

Communications

When using communication technologies the school 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.

• Users must immediately report, to the nominated person – in accordance with the school 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 6
• Any digital communication between staff and students / pupils or parents / carers (email) 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.
• pupils at KS2 will be provided with individual school email addresses for educational use.
• Pupils 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 the school website/Facebook page and only official email addresses should be used to identify members of staff.

Social Media
All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Reasonable steps to prevent predictable harm must be in place.

School staff should ensure that:
• No reference should be made in social media to pupils, parents/carers or school staff
• They do not engage in online discussion on personal matters relating to members of the school community
• Personal opinions should not be attributed to the school or local authority
• Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly by the Headteacher /Deputy Headteacher to ensure compliance with the appropriate policies.

Protecting children from the risk of radicalisation should be seen as part of schools' wider safeguarding duties, and is similar in nature to protecting children from other forms of harm and abuse. The internet and the use of social media in particular has become a major factor in the radicalisation of young people. As with other safeguarding risks, staff should be alert to changes in children's behaviour which could indicate that they may be in need of help or protection. As a school, we must ensure that children are safe from terrorist and extremist material when accessing the internet in schools.

Responding to Incidents of Misuse
It is hoped that all members of the school 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.
It is more likely that the school 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 members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour procedures.

It is important that:
Complaints of internet misuse are dealt with by a senior member of staff

- Any complaint about staff misuse must be referred to the headteacher
- Complaints of a child protection nature must be dealt with in accordance with the school's child protection procedure
- 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.

Reviewed – May 2017