St. Peter's Centre

Medical Short Stay School

Online Safety Policy

Reviewed: November 22

Aim

St. Peter's Centre identifies that the internet and information communication technologies are an important part of everyday life so children and young people must be supported to be able to learn how to develop strategies to manage and respond to risk.

The purpose of the Online Safety policy is to:

- Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use of technology to ensure that the St. Peter's Centre is a safe and secure environment
- To enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology

This policy applies to all staff including the management committee, teachers, support staff, visitors, volunteers and other individuals who work for or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as children and parents. The online safety policy will be formally provided to and discussed with all members of staff as part of induction and will be reinforced and highlighted as part of school safeguarding practice.

This policy applies to all access to the internet and use of information communication devices including personal devices or where children, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptop or mobile phone.

This policy applies to other relevant school policies including:

- SMSC
- Child Protection and Safeguarding
- Behaviour
- Staff Code of Conduct
- Whistleblowing
- Anti-bullying
- Health & Safety
- PSHE
- Risk Assessment
- Recruitment and Selection

The school's Online Safety Policy and its implementation will be reviewed at least annually or sooner if required. The School Online Safety Coordinator and the School Designated Safeguarding Lead (DSL) is the Headteacher.

Key responsibilities:

- Developing, owning and promoting the online safety vision and culture to all stakeholders in line with national and local best practice recommendations with appropriate support and consultation throughout the school community
- Auditing and evaluating current online safety practice to identify strengths and areas for improvement
- Ensuring there are appropriate and up-to-date policies and procedures regarding Online Safety
- To ensure that suitable, age-appropriate and relevant filtering is in place to protect children from inappropriate content (including extremist material) to meet the needs of the school community and ensuring that the filtering and school network system is actively monitored
- Ensuring all members of staff receive regular, up-to-date and appropriate training regarding Online Safety roles and responsibilities and provide guidance regarding safe appropriate communications
- Ensuring that Online Safety enables all pupils to develop an age-appropriate understanding of the associated risks and safe behaviours
- Making appropriate resources available to support the development of an online safety culture
- Taking responsibility for online safety incidents and liaising with external agencies as appropriate
- Receiving and regularly reviewing online safety incidents on CPOMS and using them to inform and shape future practice
- Ensuring there are robust reporting channels for the school community to access regarding online safety concerns (See anti-bullying policy)
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices
- To work with and support technical staff in monitoring the safety and security of schools systems and networks
- To ensure a member of the Management Committee is identified with a lead responsibility for supporting online safety

Key responsibilities of the designated safeguarding/online safety lead:

- Acting as a named point of contact on all online safety issues and liaising with other members of staff and agencies as appropriate
- Keeping up-to-date with current research, legislation and trends
- Coordinating participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day
- Ensure that practice is in line with legislation
- Maintaining an online safety incident/action log to record incidents and actions taken as part of the schools safeguarding recording structures and mechanisms
- Monitoring the school online safety incidents to identify gaps/trends and update the education response to reflect need and to report to the school management team, Management Committee and other agencies as appropriate
- Liaising with the local authority and other local and national bodies as appropriate
- Reviewing and updating online safety policies, Acceptable Use Rules and other procedures on a regular basis (at least annually) with stakeholder input
- Ensuring that online safety is integrated with other appropriate school policies and procedures
- Meeting regularly with the committee member with a lead responsibility for online safety

Key responsibilities of staff:

- Contributing to the development of online safety policies
- Reading the school Acceptable Use Policy and adhering to it
- Taking responsibility for the security of school systems and data
- Having an awareness of online safety issues, and how they relate to the children in their care

- Modelling good practice in using new and emerging technologies and demonstrating an emphasis on positive learning opportunities rather than focusing on negatives
- Embedding online safety education in curriculum delivery wherever possible
- Identifying individuals of concern, and taking appropriate action by working with the designated safeguarding lead
- Knowing when and how to escalate online safety issues, internally and externally
- Being able to signpost to appropriate support available for online safety issues, internally and externally
- Maintaining a professional level of conduct in their personal use of technology, both on and off site
- Taking personal responsibility for professional development in this area

Additional responsibilities for staff managing the technical environment:

- Taking responsibility for the implementation of safe security of systems and data
- To ensure that suitable access controls and encryption is implemented to protect personal and sensitive information held on school-owned devices
- Ensuring that the schools filtering policy is applied and updated on a regular basis and that responsibility for its implementation is shared with the online safety lead and DSL
- Ensuring that the use of the setting's network is regularly monitored in order that any deliberate or accidental misuse can be reported to the online safety lead and DSL.
- Report any breaches or concerns to the Designated Safeguarding Lead and ensure that they are recorded on the e Safety Incident Log and appropriate action is taken as advised
- Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure
- Report any breaches and liaising with the local authority as appropriate on technical infrastructure issues
- Ensuring that the school's ICT infrastructure/system is secure and not open to misuse or malicious attack
- Ensuring that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices
- Ensure that appropriately strong passwords are applied and enforced for all but the youngest users

Key responsibilities of children and young people:

- Reading the school Acceptable Use rules and adhering to them
- Seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues

At a level that is appropriate to their individual age, ability and vulnerabilities:

- Taking responsibility for keeping themselves and others safe online
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies
- Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks

Online safety awareness for parents:

- Reading the school's Acceptable Use Rules, encouraging their children to adhere to them, and adhering to them themselves where appropriate

- Knowing how to seek help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns

Managing the school website

- The school will ensure that information posted on the school website meets the requirements as identified by the Department for Education
- The contact details on the website will be the school address, email and telephone number; staff or pupils' personal information will not be published
- The headteacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate
- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright
- Pupils work will only be published with their permission or that of their parents/carers
- The administrator account for the school website will be safeguarded with an appropriately strong password. This is now managed by an external partner.
- The school will post information about safeguarding, including online safety on the school website

Publishing images and videos online:

- The school will ensure that all images are used in accordance with the school image use policy

Managing email:

- All members of staff are provided with a specific school email address to use for any official communication
- The use of personal email addresses by staff for any official school business is not permitted
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider
- Any electronic communication which contains any content which could be subject to data protection legislation must only be sent using secure and encrypted methods
- Members of the school community must immediately tell a designated member of staff if they receive offensive communication and this should be recorded in the school online safety incident log
- Sensitive or personal information will only be shared via email in accordance with data protection legislation
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be
- School email addresses and other official contact details will not be used for setting up personal social media accounts

Appropriate and safe classroom use of the internet and associated devices:

- The school's internet access will be designed to enhance and extend education
- All members of staff are aware that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use is essential
- Supervision of pupils is appropriate to their age and ability
- All school owned devices will be used in accordance with the school Acceptable Use Rules and with appropriate safety and security measure in place
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- The school will use the internet to enable pupils and staff to communicate and collaborate in a safe and secure environment

- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home

Social Media:

- Social networking sites are not used in school
- Safe and responsible use of social media sites will be outlined for pupils and their parents as part of the school Acceptable Use Policy/rules

Use of Personal Devices and Mobile Phones:

- Personal mobile phones and devices belonging to staff and pupils will not be used during lessons or formal school time except as part of an educational activity

Reducing online risks:

- St. Peter's Centre is aware that the Internet is a constantly changing environment with new apps, tools, devices, sites and material emerging at a rapid pace
- Emerging technologies will be examined for educational benefit and the school leadership team will ensure that appropriate risk assessments are carried out before use in school is allowed

Authorising internet access:

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications
- Parents will be informed that pupils will be provided with supervised Internet access which is appropriate to their age and ability
- Parents will be asked to read the School Acceptable Use Rules for pupil access and discuss it with their child, where appropriate
- When considering access for vulnerable members of the school community the school will make decisions based on the specific needs and understanding of the pupil(s)

Managing Information Systems:

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998
- The security of the school information systems and users will be reviewed regularly
- Virus protection will be updated regularly
- Personal data sent over the Internet or taken off site (such as via portable media storage) will be encrypted or accessed via appropriate secure remote access systems

Password protection:

- All users will be informed not to share passwords or information with others and not to login as another user at any time
- Staff and pupils must always keep their password private and must not share it with others or leave it where others can find it
- All members of staff will have their own unique username and private passwords to access school systems. Members of staff are responsible for keeping their password private
- We require staff and pupils to use STRONG passwords for access into our system

Filtering:

- The school's internet access strategy will be dependent on the need and requirements of our centre and will therefore be designed to suit the age and curriculum requirements of our pupils, with advice from technical, educational and safeguarding staff

- The school uses educational filtered secure broadband connectivity provided by RM which is appropriate to the age and requirement of our pupils
- Any material that the school believes is illegal will be reported to CEOP immediately