SS Peter and Paul Catholic Primary School

E- Safety Policy

January 2021

Includes Code of Conduct for pupils working from home

E-Safety Policy

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school 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 out of school, but is linked to membership of the school.
The school 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.

Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.
The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Aims

Education - Pupils

The education of pupils in e-safety is 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 education will be provided in the following ways:

- Provide a planned e-safety programme as part of ICT / PHSE / other lessons
- Teach pupils in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Help pupils to understand the need to sign up (annually) to the pupil Acceptable Use Policy and encourage them to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Teach pupils to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Staff to act as good role models in their use of ICT, the internet and mobile devices.

Education – Parents/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 experiences.

- The school will seek to inform parents and carers about e-safety risks and issues via parent sessions and the school newsletter.

Education & Training - Staff

- All staff receive e-safety training and understand their responsibilities, as outlined in this policy
- Help staff to understand the need to sign up (annually) to the staff Acceptable Use Policy and encourage them to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school

Technical – Infrastructure/Equipment, Filtering and Monitoring

- The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible.

Use of Digital and Video Images – Photographic, Video

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 and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees.

- The school will inform and educate users about the risks of using digital and video images and 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 e.g. on social networking sites.

Data Protection

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018

Personal data will 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 adequate protection.

Responding to incidents of misuse
It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse.
The school will aim to:

- Deal with all incidents as soon as possible in a proportionate manner
- Deal with all incidents through normal behaviour / disciplinary procedures
- Ensure that members of the school community are aware that incidents have been dealt with
- Keep an 'E-Safety Incident Log' on CPOMS of any incidents related to school and how they have been dealt with before feeding back to the Governing body at relevant meetings.

<u>Guidelines</u>
Schedule for Development/Monitoring/Review

The school will monitor the impact of the policy annually using:
- Logs of reported incidents
- SWGfL monitoring logs of internet activity (including sites visited)
- Surveys / questionnaires of
  - pupils (eg CEOP ThinkUknow survey)
  - parents / carers
  - staff

- The E-Safety policy will be reviewed annually
- Should serious E-Safety incidents occur, appropriate external agencies will be informed.

Education – Pupils

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages in the use of ICT across the curriculum.

- Rules for safe internet use should be on display in every classroom and the ICT Suite
- 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. (Hector the Protector)
- Where pupils are allowed to freely search the internet, eg using search engines, 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, pupils may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.
- Pupils 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
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Education – Parents/Carers

The school will seek to provide information and awareness to parents and carers through:

- **Termly tips/advice in weekly school newsletters**
- **Parents information evenings held at school**
- **E-Safety section of the school website**
- **Reference to the SWGfL Safe website (e.g. the SWGfL "Golden Rules" for parents)**

Education & Training – Staff

- *A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out annually.*
- *All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policy before agreeing to it*
- *This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.*
- *The E-Safety Coordinator will provide advice / guidance / training to individuals as required*

Filtering/Technical Support

The school works in partnership with parents, Bristol City Council, DfE and the South West Grid for Learning ("SWGfL") to ensure systems to protect pupils are reviewed and improved. If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the internet service provider on 0117 9037999 (cyps.it.helpdesk@bristol.gov.uk) and recorded in the E-safety log on CPoms.

Use of Digital and Video Images – Photographic, Video

- Staff 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. 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 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 pupils are published on the school website. Photographs of individual children are not to be used on the school website.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection

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, USB stick or any other removable media:

- The data must be encrypted and password protected
- The device must be password protected (many memory sticks / cards and other mobile devices cannot 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 once it has been transferred or its use is complete

Responding to incidents of misuse

- *Any incident of misuse should be reported to the E-Safety coordinator/Head teacher who in turn will take appropriate action.*

Conclusion

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (eg behaviour, anti-bullying and child protection policies).
As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

This e-safety policy helps young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

Appendix 1:

Roles and Responsibilities

The following section outlines the roles and responsibilities for E-Safety of individuals and groups within the school:

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. The role of the Safeguarding Governor will include E-Safety Governor and will monitor E-Safety within the school.

Head Teacher and Senior Leaders:

- The Head teacher is responsible for ensuring the safety (including E-Safety) of members of the school community, although the day to day responsibility for E-Safety will be delegated to the E-Safety Co- ordinator.
- The Head teacher / Senior Leaders are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their E-Safety roles and to train other colleagues, as relevant
- The Head teacher / 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.
- The Head teacher and another member 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.

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 / 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 Local Authority
- Liaises with school ICT technical staff
- Receives reports of E-Safety incidents and creates a log of incidents to inform future E-Safety developments,
- Meets regularly with the E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- Attends relevant meeting / committee of Governors
- Reports regularly to Senior Leadership Team

Network Manager:

The ICT Technician role is out sourced to the BCC It department is responsible for ensuring that:

- The school's ICT infrastructure is secure and is not open to misuse or malicious attack
- The school meets the E-Safety technical requirements
- Users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- The school's filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- The department ensures that their E-Safety technical information in order to effectively carry out their E-Safety role and to inform and update others as relevant
- The use of the network email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator /Head teacher for investigation / action / sanction
- 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
- Every year, they have read, understood and signed the school Staff Acceptable Use Policy (AUP)
- They report any suspected misuse or problem to the E-Safety Co-ordinator /Head teacher for investigation / action / sanction
- Digital communications with pupils (email / voice) 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 school activities
- Pupils understand and follow the school E-Safety and Acceptable Use Policy
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extra-curricular and extended school activities
- They are aware of E-Safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current school policies with regard to these devices
- In lessons where internet use is pre-planned 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

A member of the Safeguarding team should be trained in E-Safety issues and be aware of the potential for serious child protection 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

Pupils:

- Are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign annually before being given access to school systems
- 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 school policies on the use of mobile phones, digital cameras and hand-held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- 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

Parents/Carers:

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, website. Parents and carers will be responsible for:

- Endorsing (by signature) the Pupil Acceptable Use Policy
- Accessing the school website and apps in accordance with the relevant school Acceptable Use Policy

Appendix 2
COVID Addendum

SS Peter and Paul Code of Conduct for Remote Learning

In order to ensure that our pupils get the best out of their on-line learning we expect our learners to abide by the following code of conduct:

- I will be dressed in proper clothes to show that I am ready to do my best learning for the day. I will not wear my pyjamas.
- I will make sure that my learning environment is quiet and free from distractions
- I will make sure that the background (and foreground) of where I am working is appropriate
- I will remain attentive and focused for my learning throughout the day
- I will communicate in a polite and courteous way at all times to both my teacher and classmates
- I will be ready to start my learning by logging onto Zoom Lesson 5 minutes before the start of each session
- I will use my proper name as my user name on Zoom
- I will only use Google Classroom and my school email address for the purposes of online learning and will only browse, download, upload or forward material that is related to my learning and that is directed by my teacher
- I will not use my school email address to create groups, start calls or other meetings and will end live sessions when the teacher tells me to do so
- I will behave in a way which shows sensible learning
- During live online sessions my parent/carer will be in the vicinity, either in the room or a nearby room, with the door open
- I understand that online sessions may be recorded by my teacher but that the recordings will never be made public
- I will not take photos of my screen or record online interactions in any way
- I will not share content from Google Classroom or Zoom meetings on social media or with anyone outside of my family
- When joining in a live session with my teacher I will have my video turned on and my microphone on mute unless I need to ask a question
- I will make sure that my communications in the online learning environment are always supportive of my learning and the learning and wellbeing of others
- If I am not sure of what I need to do for my independent Remote Learning, I will ask my teacher in an appropriate and polite manner
- I will submit requested work on time
- I will always tell my parent/carer or teacher if I see, hear or read anything on the internet that upsets me or makes me feel uncomfortable. Any issues can be reported by email, phone, GOOGLE Classroom, via the office or you can report incidents to an external agency listed below.


CEOP
A National
Crime Agency
command


ChildLine
0800 1111


NSPCC
CHILD PROTECTION
HELPLINE
0808 800 5000


THINK
U
KNOW
.CO.UK