E – Safety Policy
St Anne's Preparatory School
March 2016
This policy also applies to EYFS

Introduction

It is the duty of St Anne's Preparatory School to ensure that every pupil in its care is safe; and the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and more subtle risks to young people. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking and abuse.

New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. Current and emerging technologies used in and outside of school include:

- Websites
- Email and instant messaging
- Blogs
- Social networking sites
- Chat rooms
- Music / video downloads
- Gaming sites
- Text messaging and picture messaging
- Video calls
- Podcasting
- Online communities via games consoles and
- Mobile internet devices such as smart phones and tablets

This policy, supported by the Acceptable Use Policy (for all staff, visitors and pupils), is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. It is linked to the following school policies:

- Safeguarding
- Health and Safety
- Behaviour Policy
- Anti-Bullying
- Acceptable Use / IT
- Data Protection
- PSHE&C

Whilst exciting and beneficial both in and out of the context of education, much IT, particularly online resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies.

At St Anne's School, we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom.

Both this policy and the Acceptable Use Policy (for all staff, visitors and pupils) cover both fixed and mobile internet devices provided by the school (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.); as well as all devices owned by pupils and staff brought onto school premises (personal laptops, tablets, smart phones, etc.).

Roles and Responsibilities

The e-Safety Lead (Vanessa Bridgman) has the responsibility for ensuring this policy is upheld by all members of the school community. They will keep up to date on current e-safety issues and guidance issued by organisations such as the Local Authority, CEOP (Child Exploitation and Online Protection), Childnet International and Essex Safeguarding Children Board. As with all issues of safety at this school, staff are encouraged to create a talking culture in order to address any e-safety issues which may arise in classrooms on a daily basis.

St Anne's School believes that it is essential for parents / carers to be fully involved with promoting e-safety both in and outside of school. We regularly consult and discuss e-safety with parents / carers and seek to promote a wide understanding of the benefits and risks related to internet usage.

Staff Awareness

New teaching staff receive information on St Anne's School e-Safety and Acceptable Use policies as part of their induction. All teaching staff receive regular information and training on e-safety issues in the form of INSET training and internal meeting time, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of e-safety. All supply staff, students, volunteers and contractors also receive our e-Safety Policy upon arrival at school.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. These behaviours are summarised in the Acceptable Use Policy which must be signed and returned before use of technologies in school. When children use school computers, staff should make sure children are fully aware of the agreement they are making to follow the school's IT guidelines.

Teaching staff are encouraged to incorporate e-safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community.

A record of concern must be completed by staff as soon as possible if any incident relating to e-safety occurs and be provided directly to the school's e-Safety Coordinator.

E-Safety in the curriculum and school community

IT and online resources are used increasingly across the curriculum. We believe it is essential for e-safety guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote e-safety and regularly monitor and assess our pupils' understanding of it.

The school provides opportunities to teach about e-safety within a range of curriculum areas and IT lessons. Educating pupils on the dangers of technologies that may be encountered outside school will also be carried out via PSHE, as well as informally when opportunities arise.

At age-appropriate levels, via Computing Lessons and PSHE, pupils are taught to look after their own online safety. From year 5, pupils are taught about recognising online sexual exploitation, stalking and grooming, the risks, and of their duty to report any such instances they or their peers come across. Pupils can report concerns to the Safeguarding Lead or the e-Safety Coordinator and any member of staff at the school.

From year 6, pupils are also taught about relevant laws applicable to using the internet; such as data protection and intellectual property. Pupils are taught about respecting other people's information and images (etc.) through discussion and classroom activities.

Pupils should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the school's Anti-bullying Policy). Pupils should approach the Safeguarding Lead/e-Safety Coordinator as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.

Use of school and personal devices

Staff

School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. Staff should only use the school device which is allocated to them for school work. When they are not using a device staff should ensure that it is **locked** to prevent unauthorised access.

Staff at St Anne's School are permitted to bring in personal devices for their own use. Staff are **NOT** allowed to have their phone switched on during the working day. They may use their mobile telephone during break-times and lunchtimes but **NOT** in the presence of children.
Personal telephone numbers may **NOT** be shared with pupils or parents / carers and under **NO** circumstances may staff contact a pupil or parent / carer using a personal telephone number.

Use of Internet, Email & Social Networking

Staff

Staff must not access social networking sites, personal email, any website or personal email which is unconnected with school work or business from school devices or whilst teaching / in front of pupils. Such access may only be made from personal devices whilst not in the presence of children.

When accessed from personal devices / off school premises, staff are requested to use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position.

There is strong anti-virus and firewall protection on our network and, as such, it may be regarded as safe and secure. Staff should be aware that email communications are monitored.

Staff must immediately report to the e-Safety Coordinator 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 online communications must not either knowingly or recklessly:

- place a child or young person at risk of harm
- bring St Anne's School into disrepute
- breach confidentiality
- breach copyright
- breach data protection legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:

    1. making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
    2. using social media to bully another individual; or
    3. posting links or material which is discriminatory or offensive.

Under no circumstances should school pupils or parents be added as social network 'friends'. Staff must not post pictures of school events without the Head Teacher's consent.

Any digital communication between staff and pupils or parents / carers must be professional in tone and content. Under no circumstances may staff contact a pupil or parent / carer using any personal email address. The school ensures that staff have access to their work email address when offsite, for use as necessary on school business.

Pupils

All pupils are issued with their own personal school e-mail addresses for use on our network [and by remote access]. Access is via a personal login, which is password protected. This official email service may be regarded as safe and secure, and must be used for all school work, assignments / research / projects. Pupils should be aware that email communications are monitored.

There is strong anti-virus and firewall protection on our network. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for school work / research purposes, pupils should contact IT Lead for assistance.
Pupils should immediately report, to the e-Safety Lead (Vanessa Bridgman) or another member of staff 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.

Pupils must report any accidental access to materials of a violent or sexual nature directly to the e-Safety Lead or another member of staff. Deliberate access to any inappropriate materials by a pupil will lead to the incident being recorded on their file and will be dealt with under the school's Behaviour Management Policy.

Pupils should be aware that all internet usage via the school's systems and its wifi network is monitored.

Certain websites are automatically blocked by the school's filtering system. If this causes problems for school work / research purposes, pupils should contact IT Lead for assistance.

Data storage

The school takes its compliance with the Data Protection Act 1998 seriously. Please refer to the Data Protection Policy and the Acceptable Use Policy for further details.

Staff and pupils are expected to save all data relating to their work to the school's central server as per the IT Policy.

One Drive is to be used to transport school data between home and school. USB memory sticks, CD's, portable drives should not be used to transport school data.

Staff may only take information offsite when authorised to do so, and only when it is necessary and required in order to fulfil their role.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the e-Safety Lead.

Password Security

Pupils and staff have individual school network logins, email addresses and storage folders on the server. Staff and pupils are regularly reminded of the need for password security.

All pupils and members of staff should:

- use a strong password (usually containing eight characters or more, and containing upper and lower case letters as well as numbers), which should be changed every six weeks. (Zen Zero will set reminders on profiles to remind staff)
- not write passwords down; and
- should not share passwords with other pupils or staff

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, stalking or grooming 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.

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).

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 is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published on blogs or social networking sites (etc.), unless permission has been obtained from the parents' concerned; nor should parents / carers comment on any activities involving other pupils in the digital / video images.

Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow this policy and the Acceptable Use Policy / IT Policy concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment: personal equipment should **NOT** be used for such purposes. Class camera's must be kept in a safe and secure place and stored away each evening.

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.

Written permission from parents or carers will be obtained before photographs of pupils are published on the school website (see Parent Contract / Acceptable Use Policy for more information).

Photographs published on the school website, or displayed 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.

Use of mobile phones by members of staff, volunteers and visitors to the school

It is the school's responsibility to ensure that pupils and staff are safeguarded in relation to the potential for improper use and also that pupils' education is not impeded by the use of mobile phones at inappropriate times.

Many mobile phones have inbuilt cameras therefore staff mobile phones must not be carried around in pockets and should be left with personal belongings. Staff are asked to only use their mobile phones in the staff room or other location when there are no children present. This does not apply when offsite, where discretion is needed regarding making and receiving important school-related calls, the school mobile phone will be used when offsite.

Staff must be vigilant to ensure that the use of mobile phones, including their use by volunteers and visitors to the school is always appropriate and the safeguarding needs of the pupils are met. Visitors should only use their phone outside the building and should be challenged if seen using their phone inappropriately or taking photographs of children. Any concerns should be discussed with the DSL, (Vanessa Bridgman). Concerns will be taken seriously, logged and investigated appropriately.

Under no circumstances must a personal mobile phone be used by staff, volunteers or visitors to take photographs of children in the school setting.

Staff will **NOT** use personal mobile numbers to contact parents.

Complaints

As with all issues of safety at St Anne's School, if a member of staff, a pupil or a parent / carer has a complaint or concern relating to e-safety, prompt action will be taken to deal with it. Complaints should be addressed to the e-Safety Coordinator in the first instance, who will undertake an immediate investigation and liaise with the Senior Management team and any members of staff or pupils involved. Please see the Complaints Policy for further information.

Incidents of or concerns around e-safety will be recorded using a Record of Concern form/Incident Report form and reported to the school's e-Safety Lead and the Designated Safeguarding Lead, Vanessa Bridgman, in accordance with the school's Child Protection Policy.