# ***E-Safety Policy***

## Development of The Policy

This policy has been developed by the E-Safety committee of St Paul's Primary School using publications from Manchester Safeguarding Children Board (MSCB), South West Grid for Learning, Kent Local Education Authority and Government Advice, and through consultation with
•Staff
•Governors
•Parents
•Pupils

This policy will be reviewed annually, or more regularly in the light of any significant development in the use of the technologies, new threats to e-safety or incidents that have taken place. The anticipated next review date will be December 2014.

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

## Background and Rationale

Internet technologies are becoming an increasingly integral part of young people's lives. Many children make routine use of such technologies to develop their understanding of the world and to communicate with others. Furthermore, the use of such innovative and exciting technologies can have a positive impact on pupils' level of engagement and their 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
- Unauthorized 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 risk of being radicalized by terrorists or extremist groups
- 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.

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 (e.g. 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 students'/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.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues to help young people (and their parents/carers) to be careful, considerate and safe users of online technologies.

## Scope of Policy

This policy applies to all members of the school 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 the school.

## 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 its effectiveness. This will be carried out by regular reports to the Governors (or relevant committee) about e-safety training, incidents and monitoring. A member of the governing body should be appointed as E-Safety Governor, this role will include:

- Attending regular meetings with the E-Safety Coordinator
- Monitoring of the E-Safety logs
- Reporting to relevant Governors' meetings

### Head-teacher - (E-Safety Coordinator)

The head-teacher is responsible for ensuring the safety (including e-safety) of members of the school community by

- Ensuring that staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- Ensuring 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.
- Taking a day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies and documents (including AUP's and risk assessments).
- Ensuring that all staff are aware of the procedures that need to be followed in event of an e-safety incident taking place
- Leading the e-safety committee
- Acting as a single point of contact for both MSCB and agency staff and agency staff and service users.
- Making appropriate responses to policy breaches and ensure correct execution of reporting procedures including escalating incidents with external agencies as appropriate.
- Ensuring that an e-safety education curriculum is being delivered

### ICT Coordinator (TLR Post)

The ICT coordinator is responsible for assisting the head teacher (e-safety coordinator) in all aspects of e-safety by

- Providing training and advice for staff
- Receiving, recording, monitoring and reviewing incidents of e-safety to inform future e-safety developments
- Meeting regularly with the E-Safety Coordinator to discuss current issues and review incident logs.
- Developing and updating a relevant e-safety curriculum
- Overseeing the school's technical support provision to ensure that their roles are adhered to.

**Technical Support Staff**

Through partnership with the school's ICT coordinator, the school's technical support staff is responsible for ensuring that:

- the school's technical infrastructure is secure and is not open to misuse or malicious attack
- the school meets the the Local Authority's online safety technical requirements
- they keep up to date with recent e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- the school's network is regularly monitored so any attempted misuse can be reported to the E-Safety Coordinator
- anti-virus, filtering and security software are up to date

**Teaching and Support Staff**
Are responsible for supporting the school's E-Safety work by

- Having an up to date awareness of e-safety matters and of the current school e-safety policy and practices.
- Ensuring they have read, understood and signed the school Staff Acceptable Use Policy (AUP) Agreement
- Reporting any suspected misuse (including incidents of an accidental nature) of the school's ICT network (including associated hardware) or incidents of cyber-bullying to the E-Safety Coordinator.
- Embedding e-safety issues in all aspects of the curriculum and other school activities
- Ensuring pupils understand and follow the school e-safety and acceptable use policy
- Monitoring ICT activity in lessons, extra-curricular and extended school activities
- Checking the content of websites and web-based media (downloaded or streamed) that they intend to use with pupils before the lesson to assess suitability and make sure processes are in place for dealing with any unsuitable material.
- Checking and monitoring the use of ICT by visitors to the classroom to ensure that content is appropriate for the pupils and is in line with the E-Safety policy.

**Designated person for child protection**
Should be trained in e-safety issues and be aware of the potential for serious child protection issues that could 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

**E-Safety Committee**
Members of the E-safety committee (or other relevant group) will assist the E-Safety Coordinator by:

- supporting the development / reviewing / monitoring of the school e-safety policy / documents.

**Students / pupils:**

- Are responsible for using the school ICT systems in accordance with the Pupil AUP Agreement.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and incidents of cyber-bullying and know how to do so

- 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.

**Parent/Carers**

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' sessions, newsletters, letters, website / Learning Platform and information about national/local online safety campaigns/literature.

**Community Users**

Community Users who access school systems as part of the wider school provision will be expected to sign a Community User AUP before being provided with access .

## E-Safety Curriculum

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of spupils in online safety is therefore an essential part of the school's online safety provision. Children need the help and support of the school to recognise and avoid online safety risks and build their resilience. Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online 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 program will be provided as part of computing lessons – this will cover both the use of ICT and new technologies in school and outside school and will be based on the SMART internet rules developed by *Childnet* and resources from CEOP via the *thinkuknow* website.
- Key e-safety messages should be embedded into other areas of the curriculum.
- Issues arising from reported e-safety issues, including cyber-bullying, will be addressed in assemblies, with year groups or individual pupils as appropriate.
- Pupils should be taught in all lessons to be critically aware of the reliability of information found on the internet.
- Pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Rules for use of ICT systems/internet will be posted in classrooms.
- Staff should act as good role models in their use of ICT, the internet and mobile devices

## E-Safety Training

It is essential that all staff receive e-safety 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. An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies.

- The E-Safety Coordinator will receive regular updates through the attendance of MSCB meetings and by reviewing national and local guidance documents.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings.
- The E-Safety Coordinator will provide advice/guidance/training as required to individuals

Governors

Governors should take part in e-safety training/awareness session. The E-Safety Coordinator will provide training for all governors.

## Technical Information

The school will be responsible for ensuring that the school network (including associated hardware) is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. To allow for this to happen the following steps will be taken:

The School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the MSCB E-Safety Guidelines.

- The school will use a Local Authority approved Internet Service Provider and filtering system.
- All technologies will be risk-assessed with regard to e-safety
- There will be regular reviews and audits of the safety and security of school ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the ICT Coordinator and will be reviewed, at least annually, by the E-Safety Committee.
- All staff will be provided with a username and password that they must not divulge to others. The ICT Coordinator will keep an up to date list of staff users names. Staff are responsible for notifying the ICT Coordinator if they change their password
- All pupils (at KS1 and above) will be provided with a username which they must not share with other pupils
- The “master/administrator” passwords for the school ICT system, used by the ICT Technical Staff must also be available to the Headteacher.
- In the event of the ICT Technical Staff (or another person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher.
- Requests from staff for sites to be removed from the filtered list will be considered by the E-Safety Coordinator. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly by the E-Safety Committee
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- An appropriate system is in place for users to report any actual / potential e-safety incident to the Network Manager (or other relevant person).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.

In addition to the aforementioned steps, members of staff are responsible for ensuring the school's ICT infrastructure is not comprised by

- Only ever using their individual username and password to access the school's network and logging off when the have finished their session.
- Only ever using hardware provided by the school with the school's ICT infrastructure.
- Never connecting school hardware to any personal device whether in school or at home. If documents completed on a personal computer are needed for work purposes they should be emailed to your school address and downloaded on site.

## Staff Wireless Devices

The wireless devices (laptops, iPads, tablets etc) provided by the school remain the property of the school at all times. As these items are entrusted to certain individuals an additional set of rules govern these items.

- Any member of staff who has been given a wireless device must sign the wireless device contract.
- The device must always be in school when the associated staff member is in school.
- The device may be taken off-site for work-related activities.
- The device may be connected to a **wireless** home network
- Personal USB based hardware (cameras, pen drives, external hard drives etc.) must not be connected to the device.
- The associated member of staff is responsible for the use of the device, at all times, while it is off-site.
- Files must be stored on the the provided encrypted pen drive
- Personal files must not be stored on the device (this includes images and media files)
- Sensitive pupil or staff data must not be stored on any portable memory device.
- The ICT coordinator will keep a record of all encrypted pen-drive passwords.
- Permission from the ICT coordinator must be sought before installing any new software application. Updating existing applications (new smart notebook, flash etc) is allowed.
- The device may be used for personal internet use (including forms of internet communication) providing that it does not contradict any of the rules set out in this e-safety document.
- Any infringements of these rules, regardless of who has carried out the action, must be reported to the school's e-safety coordinator as soon as possible.

## 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 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.

- 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.
- Images should be stored on a password protected drive on the school's network, access to this drive is limited to school staff.
- Digital images must be uploaded and deleted from media cards at the first opportunity.

- Staff are allowed to take digital / video images to support learning, but must follow school policies concerning the sharing, distribution and publication of those images. Whenever possible the images should be recorded using school equipment. However, in cases where this is not possible staff may use smartphones but must ensure that the files are transferred to the school's network and deleted from the personal device at the earliest possible opportunity.
- Members of staff must be able to justify the reasons behind taking and storing any digital media file (including image and sound).
- 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 share, publish or distribute images of others.
- When taking photos, staff should ensure that there is more than one pupil in the picture.
- Photographs published on internet-based platforms that include pupils will be selected carefully and will comply with good practice guidance on the use of such images. Text that accompanied such images will not name any child ***example – year five pupils enjoying a music lesson.*** On certain occasions, it will be necessary to publish pictures of individual children, whether this be on the internet or in school. The school will always seek permission of the parents/carers of these pupils before the images are displayed.
- Written permission from parents or careers will be obtained before images of pupils are taken and uploaded to on any internet-based platform. An up-to-date list is kept in the office it is the responsibility of the person recording the images to check the list.

## The School's' Website (ww.stpaulswithington.co.uk)

St Paul's uses its website to celebrate successes, share information and keep parents/carers informed about events taking place. Furthermore, the school's website also provides information about the school's curriculum and performance data.

Certain sections of the school website are restricted to authorized users. All parents/carers known to the school, who wish to be a authorized users, will be given a unique username and password. The school keeps an up-to-date list of usernames and passwords. The website administrator is able to track the action of all authorized users while logged in.

## The Use of You-Tube

The school has unblocked the video-sharing site you-tube to allow teachers and pupils to benefit from the rich variety of educational content that it offers. However as the site is also used to share videos socially the following rules must be adhered to, to help ensure the safety of the pupils and the integrity of the school's network

- All staff must complete training (relating to the points below) and sign the you-tube AUP before accessing you tube in school in any capacity.
- Staff have access to you-tube to support teaching and learning, personal use of youtube is allowed before 8.30am and after 3.30pm but use must be appropriate to the environment in which they work. This rule applies regardless of the device/network used to connect to youtube.
- Teachers must not search for videos in front of the class; all videos must be found prior to the lesson.
- As youtube videos do not come with age classification advice, teachers must watch the entire video to assess the suitability of the resource for the pupils they teach.
- Teachers must be aware that you-tube is a commercial site and that videos may contain adverts. If adverts are displayed as part of the video it is suggested that the commercial nature of the site is discussed with the class

- Pupils are not allowed to use you-tube on their individual devces; any videos that they need to be watched to support their learning, should be shown to the entire class through the room's projector.
- If an inappropriate video/image is displayed, the screen should be turned off and the incident reported to the head-teacher or ICT subject leader as soon as possible.

## The Use of Twitter

The school uses Twitter as an additional tool to promote parental engagement by sharing photos and information about events, activities and success' of the pupils. Examples of the use so far: pictures of artwork completed by the class; pictures of classroom displays; pictures of children learning to ride bikes. To ensure the staff use of twitter is consistent with the rules already laid out within the policy they must adhere to the rules below.

- All staff must undertake training (relating to the points below) and sign this twitter AUP before using twitter in school.
- Any staff member who wishes to use twitter will be given an address that identifies them as a member of the school (eg @mrdstpaulspri). This account must only be used in a professional context. The accounts members of staff follow must be appropriate to the environment in which they work.
- The twitter account must be registered to your school email address @st-pauls-pri.manchester.sch.uk
- An image of the school's badge is to be used as a profile picture.
- The school will keep a record of every user name and password.
- Personal twitter accounts must not be linked to school twitter accounts.
- Images, including those of pupils, can be tweeted but must adhere to the digital images section of the school's e-safety policy.
- Staff are responsible for checking the content and the appropriateness of any websites they post links to.
- Staff must be aware that all messages/tweets can be seen by anyone accessing the twitter web platform.
- Teachers should not enter into dialogue with anyone through twitter.

## Communications

A wide range of rapidly developing communications technologies have the potential to enhance learning. This section details the technologies the school currently allows the use of and the manner in which they should be used.

- All staff will be provided with a school email address, which is to be used solely for communication regarding their job. Users need to be aware that email communications may be monitored. You should only use your email address to register to website that are of an educational basis and not for personal social media sites.
- The school regularly communicates with the staff through email, it is therefore expected that staff check their email daily.
- Staff may only access personal email before 8.30am and after 3.30pm, this rule must be adhered to when on the school premises regardless of the device that is being used to connect.
- Attachments emails should only be opened if they are from known sources and never on personal email.
- Children are prohibited from using mobile phones within school although the school will allow pupils to bring a mobile phone to school, which needs to be left in the school office. If parents/carers wish their children to bring a mobile phone to school, they must inform the school in writing and understand that the school accepts no responsibility for any damage that may occur to these phones while in the school's possession.

- All users must immediately report, to the E-Safety Coordinator, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Parents may use official email addresses to contact members of staff. Under most circumstances, the staff should reply to emails through a letter on school headed paper. If the response to the email is presenting simple facts (times of swimming lessons) then an email response is permitted but a carbon copy (cc) of the email must be send to head@st-pauls-pri.manchester.sch.uk.
- Staff should be aware that under the freedom of information act all emails are subject to disclosure (to any party) and can be used in a court of law if required.
- Any digital communication between staff and pupils must be professional in tone and content. These communications may only take place on official (monitored) school web applications and messages **should not be private**. The use of any other form of digital communication (including personal accounts) is strictly prohibited.
- Students / pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website.

## Staff Use of Mobile Phones

Although mobile phones are an essential personal communication tool, they also provide a distraction for both staff and pupils. To minimise the disruption to learning all teaching staff (teachers, teaching assistants) need to follow the below rules.

Mobile phones should be switched off or to silent and placed out of sight during teaching times, regardless if you are working with pupils or preparing resources.

Personal phone calls should only be made before school, at break and lunchtimes, or after school and should take place in the staffroom or an empty classroom. **No** member of staff should be walking around school using their mobile phone.

While the use of the mobile internet network is allowed, staff must only access websites, and website based apps (facebook), that are consist with the rules set out in this document.

If a member of staff needs to leave his/her mobile phone on because he she is expecting an urgent phone call, he/she must inform their team leader before doing so.

## Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other ICT systems. Other activities e.g. Cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

The school 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. Users shall not visit Internet sites, make posts, download, upload, data transfer, communicate or pass on, materials, remarks, proposals or comments containing or relating to:

- Child sex abuse images
- Promotion or conduct of illegal acts
- Adult material that potentially breaches the Obscene Publications Act in the UK
- Criminal racist material in the UK
- Terrorists or extremist groups
- Pornography

- Promotion of any kind of discrimination
- Threatening behaviour, including the promotion of physical violence or mental harm
- Any other information that may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute
- Running a private business
- Systems, applications, websites or other mechanisms that by pass the filtering or other safeguarding employed by the local authority or the school
- Uploading or downloading or transmitting commercial software or any copyrighted materials belonging to third party, without necessary licensing permissions
- Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Personal social network sites
- Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet
- Gambling sites
- File sharing

**This list must be adhered to regardless of the device used to connect to the internet**.

## Use of Social Media

While the school cannot govern the individual's use of internet-based social media outside of the school, it does expect all members of staff to uphold the profession and the institution by using these sites in a responsible manner, exercising common sense at all times. To help do so, staff are advised:

- To use security settings to restrict access to their accounts including view, searching and tagging.
- Not to upload pictures of school events (both official and unofficial).
- Not to post status updates regarding events in school and don't enter into discussions with others regarding school.
- Not to accept any pupils (existing or past) or parents as friends.
- Remember comments made in writing are subject to disclosure and could be used as evidence in a court of law.

## Monitoring and reporting

In accordance with MSCB policy the school will monitor its network regularly and consistently. All users will be made aware of this through the AUP.

Maintain an incident log of e-safety incidents, including cyber-bullying that include:

- A description of the event
- Details of people involved
- How the incident was identified
- What actions were taken
- Conclusion of the incident

## Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

Any breach of the E-Safety policy will be responded to in accordance to MSCB Incident Response Form and will be recorded in the school's e-safety log.

In situations where the pupils have been the perpetrators the school will use the consequences set out in its behaviour policy in addition to any other sanctions.

In the event of a serious breach of the E-Safety policy a full review of the E-Safety and Acceptable Use policies and procedures will be conducted as soon as possible by the E-Safety Committee.

**I understand that I am responsible for my actions in and out of school:**

- I understand that the E-Safety Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the St Paul's CE Primary School's E-Safety Policy and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

| | |
|---|---|
| Staff Name | |
| Signed | |
| Date | |