E SAFETY POLICY

St Philip Westbrook C of E Aided Primary School

Date of Review	Action
MAY 2015	Agreed with Governors
MAY 2016	Agreed with Governors
MAY 2017	

E SAFETY POLICY

SCOPE OF THE POLICY

This policy applies to all members of St Philip Westbrook CE Aided Primary School community (including staff, pupils, volunteers, parents / carers, visitors, church, community users) who have access to, and are users of the school ICT system.

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

St Philip Westbrook will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

To highlight the importance of these policies all staff must sign their written understanding and agreement with the school office at the beginning of each academic year or when changes occur.

This policy MUST be read in conjunction with the Acceptable Use Policy, it also links to:

- Staff Conduct
- Safeguarding
- Behaviour
- Anti-Bullying
- Data Protection

CONTENTS OF THE POLICY:

ROLES AND RESPONSIBILITIES

The following section outlines the e-safety roles and responsibilities of individuals and groups within St Philip Westbrook CE Aided Primary School.

GOVERNORS:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy with the support of the E Safety Governor. A member of the Governing Body has taken on the role of E-Safety Governor.

The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Co-ordinator
- regular monitoring of e-safety incident logs
- reporting to relevant Governors

HEADTEACHER AND SENIOR LEADER:

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator.
- The Headteacher 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. (See appendices).
- The Headteacher is responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Senior Leadership Team will receive regular monitoring reports from the E-Safety Co-ordinator.

E-SAFETY COORDINATOR:

The named member of staff for E Safety Coordinator is Angela Deakin (Deputy Head teacher) and:

- leads the e-safety committee
- 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 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 technician logs
- reports regularly to Senior Leadership Team

TECHNICAL STAFF:

The E Safety Co-ordinator is responsible for ensuring that (in liaison with MGL):

- the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- the school meets required e-safety technical requirements and any Local Authority E-Safety Policy / Guidance that may apply.
- users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- they keep up to date with 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 / internet / remote access / is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher & E-Safety Coordinator for investigation / action / sanction.
- monitoring 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
- they have read, understood and signed the staff E Safety and Acceptable Use Policies / and Staff Conduct Policy
- they report any suspected misuse or problem to the Headteacher / Senior Leaders / E-Safety Coordinator for investigation / action / sanction
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using the official school office email, phone calls or in person
- e-safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the E-safety Rules and Acceptable Use Policy
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they 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
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that any unsuitable material found in internet searches is recorded in the Behaviour Log. Pupils should switch their monitor off immediately if this occurs and report it to a member of staff.

SAFEGUARDING DESIGNATED PERSON

should be trained in e-safety issues and be 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

E-SAFETY GROUP

The E-Safety Group provides a consultative group that has wide representation from the school community, with responsibility for issues regarding e-safety and the monitoring of the e-safety policy, including the impact of initiatives. The group will also be responsible for regular reporting to the Governing Body.

Members of the E-safety Group will assist the E-Safety Coordinator with:

- the production / review / monitoring of the school e-safety policy / documents.
- mapping and reviewing the e-safety curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the students / pupils about the e-safety provision
- monitoring improvement actions identified through use of the 360 degree safe self-review tool

PUPILS:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy
- 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
- 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. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, the school website and information about national / local e-safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website
- their children's personal devices in the school
- the schools Acceptable Use Policies

COMMUNITY USERS

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

EDUCATION & TRAINING

PUPILS

The education of pupils in e-safety is an essential part of the school's e-safety provision.

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 and will be provided in the following ways:

- A planned e-safety curriculum provided as part of Computing / PHSE / lessons across the curriculum and regularly revisited
- Key e-safety messages reinforced as part of a planned programme of assemblies
- Pupils 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 taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff acting as good role models in their use of digital technologies, the internet and mobile devices
- In lessons where the internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use , if any unsuitable material is found pupils should switch off the monitor and inform a member of staff.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

PARENTS AND 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 behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to assist parents and carers through:

- curriculum activities
- letters, newsletters, website,

- parents / Carers evenings / sessions
- high profile events / campaigns e.g. Safer Internet Day
- reference to the relevant web sites / publications

THE WIDER COMMUNITY

The school will provide opportunities for local community groups to gain from the school's e-safety knowledge and experience. This may be offered through the following:

- E-Safety messages targeted towards grandparents and other relatives as well as parents.
- The school website provide e-safety information for the wider community
- Supporting community groups e.g. Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their e-safety provision (possibly supporting the group in the use of Online Compass, an online safety self-review tool - www.onlinecompass.org.uk)

STAFF / VOLUNTEERS

Staff will receive e-safety training and must understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- All new staff will receive e-safety training as part of their Safeguarding training, staff must ensure that they fully understand the school E-safety and Acceptable Use Policies.
- The E-Safety Coordinator will receive regular updates through attendance at external training events (e.g. LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The E-Safety Coordinator will provide advice / guidance / training to individuals as required.

GOVERNORS

Governors will take part in e-safety training / awareness sessions, with particular importance for those who are members of any subcommittee group involved in technology / e-safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation.
- Participation in school training / information sessions for staff or parents.

TECHNICAL – INFRASTRUCTURE, EQUIPMENT, FILTERING & MONITORING

The school will ensure that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- All staff will have an individual user name and secure password for the system. Pupil users will be provided with a class log on for the system and an individual user name and password for Purple Mash. E Bright (Support staff and E Safety Group member) will keep an up to date record of pupil users and their usernames for Purple Mash.
- MGL is responsible for ensuring that software licence logs are accurate, up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users by the Local Authority.
- Any actual / potential technical incident / security breach should be reported to the E Safety Coordinator and the Behaviour Log completed. This will be monitored.
- The school's infrastructure and individual workstations are protected by up to date virus software.
- Guests (e.g. trainee teachers, supply teachers, visitors) who are DBS checked are given temporary access via a temporary log on onto the school systems in liaison with the E Safety Coordinator and MGL. Users are required to read and sign the Acceptable Use Policy.
- Teachers are able to take their laptops and teacher iPad home, providing they are password protected and do not contain any images / videos of children.
- Staff should not download executable files or install programs on their laptop. Staff may temporarily install Apps on their iPad to test out in liaison with MGL. These should then be deleted, or installed by MGL across the Unit iPads.
- Guests / children must have their memory sticks scanned by the office prior to usage in school to prevent viruses.
- Only memory sticks / CDs / DVDs that have been purchased by the school may be used on school systems by staff. Encrypted memory sticks with tracking data may be taken home but files must be deleted from them as soon as they are no longer needed.

USE OF DIGITAL AND VIDEO IMAGES

Staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet.

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 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 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 pupils in the digital / video images.
- Staff (not volunteers) are allowed to take digital / video images to support educational aims. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes. School equipment containing images of children, e.g. iPads, cameras, laptops, should never be taken from the school premises.
- 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 used elsewhere that include pupils will be selected carefully and will comply with this policy.
- Pupils' full names will not be used anywhere on the public 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.

ELECTRONIC DATA PROTECTION

In line with the Data Protection Policy, staff must ensure that they:

- At all times take care to ensure the safe keeping of school 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.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the device must have a password
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, once it has been transferred or its use is complete

COMMUNICATIONS

A wide range of rapidly developing communications technologies has the potential to enhance learning:

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure. Users should be aware that email communications are monitored.
- Users must immediately report 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 digital communication between staff and pupils or parents / carers (official school email or telephone only) must be professional in tone and content. These communications may only take place on official school systems or email addresses. Personal email addresses, text messaging or social media must not be used for these communications.
- Children should not have access to any email communication.
- 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. and only official email addresses should be used to identify members of staff.

SOCIAL MEDIA

- School staff should ensure that they follow the agreements in the School Acceptable Use Policy.
- Only those authorised by the school are permitted to give media statements. Any press enquiries should be directed to the Headteacher.

The school's use of social media for professional purposes will be checked regularly by the e-safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Breach of this policy is a disciplinary offence and may lead to action under the school's disciplinary policy, which potentially constitute gross misconduct and may lead to dismissal.

CLOUD BASED STORAGE

Cloud based storage systems should not be used to store any personal information or photographs unless approved by the Headteacher.

MOBILE PHONES

Children may bring mobile phones to school but these must be passed to the school office at the start of day and collected at the end of the day. These phones should not be used anywhere on the school premises.

Staff may use mobile phones on school/trips/residentials but only when there are no children present. Mobile phones should be kept out of reach and sight at all other times. The school mobile phones should be used on trips/residentials to contact parents rather than personal phones.

ELECTRONIC DEVICES – SEARCHING AND DELETION

The school reserves the right to search for/search any device that is against school policy, remove the device and delete the data (and/or retain a copy).

Pupil Acceptable Use Agreement – Junior Children

- I understand that I must use the internet and school devices in a responsible way.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password.
- I will follow the school e safety rules (SMART)
- I will immediately report anything that makes me feel uncomfortable when I see it on-line.
- I will be polite and responsible when I communicate with others at home and at school. I understand that I will receive consequences if I make inappropriate comments about school, staff or other pupils.
- If I need a mobile phone I will ensure that it goes to the school office at the start of the day and collect it at the end. I will not use my phone anywhere on school property.
- I will not access on-line gaming, social network sites, or any other site that I know is unsuitable for use at school.
- When I am using the internet to find information, I will take care to check that information is accurate.
- I understand that I must follow these rules when I am out of school.
- I understand that if I do not follow this Acceptable Use Policy Agreement my parent/carer will be contacted and that I will receive consequences.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

I have read and understand the above and agree to follow these guidelines when:
- I use the school systems and devices (both in and out of school)
- I bring my mobile to school
- I use my own equipment out of the school in a way that is related to me being a member of this school and its rules.

Name of Pupil	
Group / Class	
Signed	
Date	
Parent / Carer Countersignature	

Pupil Acceptable Use Policy Agreement Reception, Y1 & Y2

This is how we stay safe when we use computers:

I will follow the school e safety rules (Sid's Top Tips).

I will only use activities that a teacher has told or allowed me to use.

I will take care of the computer and other equipment.

I will ask for help from a teacher or adult if I am not sure what to do or if I think something has gone wrong.

I will tell a teacher or adult if I see something that upsets me on the screen.

I know that if I break the rules I might not be allowed to use a computer.

Signed (child):……

Signed (parent): ……..

Parental Consent - Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media.

The school will comply with the Data Protection Act and request parents / carers permission before taking images of pupils in the school. We will also ensure that when images are published that the pupils cannot be identified by the use of their names.

Parents / carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites or the internet.

Parents / carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents / carers to agree.

Digital / Video Images Permission Form

Parent / Carers Name	
Student / Pupil Name	

As the parent / carer of the above pupil, I agree to the school taking and using digital / video images of my child / children to support learning.	Yes / No
I agree to the images/video being used on the school website, names will not be used.	Yes / No
I agree to the images/video being used on the school Twitter account, names will not be used.	Yes / No

I agree that if I take digital or video images of school events, which include images of children other than my own, I will not make them public or publish online.

Signed	
Date	