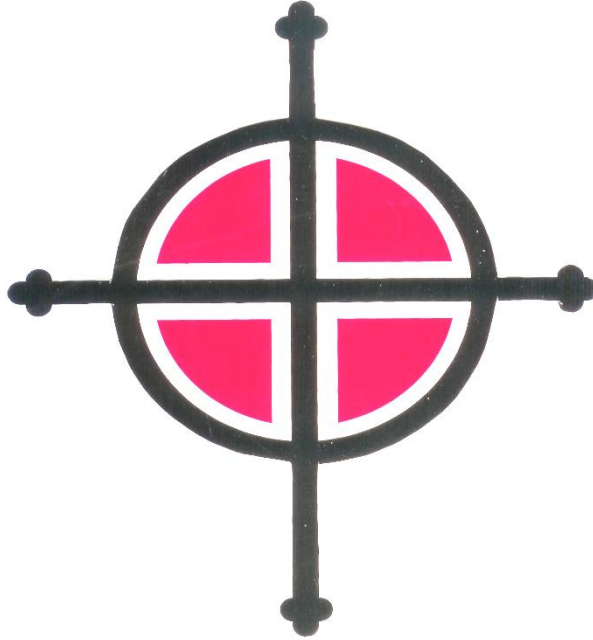


# E-SAFETY POLICY



## St Philip Westbrook C of E Aided Primary School

Date of Review	Action
JANUARY 2018	Reviewed and updated

## **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.

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

- Staff Conduct
- Safeguarding
- Behaviour
- Anti-Bullying
- Data Protection
- Mobile Phone & Devices Policy

### **CONTENTS OF THE POLICY:**

Pg. 2	Roles and Responsibilities
Pg 5	Education and Training
Pg 6	Technical Infrastructure, Equipment, Filtering and Monitoring
Pg 7	Use of Digital and Video Images
Pg 7	Mobile Phones
Pg 7	Electronic Devices Searching and Deletion
Pg 8	Acceptable Use for Infant Children
Pg 9	Acceptable Use for Junior Children
Pg 10	Parental Consent for the Use of Digital and Video Images

## **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 associated policies 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 Champion
- regular monitoring of e-safety incident logs & filtering reports
- reporting to relevant governors

### **HEADTEACHER AND SENIOR LEADERS:**

- 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 Champion.
- 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.
- The Headteacher is responsible for ensuring that the E-Safety Champion 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 Champion.

### **E-SAFETY CHAMPION:**

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

- 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 the e-safety curriculum is reviewed and updated in line with guidance
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school technical staff
- monitors reports of e-safety incidents to inform future e-safety developments & provide guidance and support
- meets regularly with the E-Safety Governor to discuss current issues, review incident logs, policies & filtering logs
- reports regularly to the Senior Leadership Team

## **TECHNICAL STAFF:**

The E-Safety Champion is responsible for liaising with MGL/Warrington Borough Council to ensure that:

- 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 are provided with passwords to access the school network
- the use of the network is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation / action / sanction

## **TEACHING AND SUPPORT STAFF**

Teachers and Teaching Assistants are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school E-Safety Policy, Acceptable Use Policy, and associated policies and practices
- they have read and understood the associated policies listed at the start of this policy including the Acceptable Use policy
- they report any suspected misuse or problem to the Headteacher / senior leaders / E-Safety Champion for investigation / action / sanction
- e-safety is specifically taught within Computing and PSHE, and embedded in all aspects of the curriculum and learning
- pupils understand and follow the school's e-safety rules (SID's Top Tips & SMART rules) and children's Acceptable Use Policy
- pupils switch their screen off/close laptop lid immediately if any unsuitable material appears and report it to a member of staff

## **SAFEGUARDING - SENIOR DESIGNATED PERSON**

The SDP should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues including for example:

- sharing of personal data & managing online information
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- radicalisation
- privacy and security
- cyber-bullying

## **PUPILS:**

Pupils:

- are responsible for using the school technology systems in accordance with the Pupil Acceptable Use Policy
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should understand the rules for safe online use: SID's top tips for infants and SMART rules for juniors
- follow e-safety teaching and learning in school and at home
- 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 and carers play a crucial role in ensuring that their children understand the need to use the internet / devices in an appropriate and positive way.

Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow advice including:

- security settings, privacy and parental controls
- safely using the internet/devices at home in line with SID's top tips and SMART rules
- digital and video images taken at school events
- their children's personal devices in the school
- the school's Acceptable Use Policies for children
- online conduct and reputation
- copyright and ownership
- accessing age appropriate online content
- online contact and grooming
- important conversations
- promoting positive health, wellbeing and lifestyle

## **COMMUNITY USERS**

Community Users who access school internet as part of the wider school provision will be expected to sign a Community User Acceptable Use Agreement before being provided with access.

## **EDUCATION & TRAINING**

### **PUPILS**

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

The e-safety curriculum is broad, balanced, relevant and ensures progression across school. The curriculum will be reviewed regularly in order to take account of new e-safety issues, up to date guidance and new technology. It aims to empower, build resilience and ensure the development of long term safe behaviours.

It will be provided in the following ways:

- A planned e-safety curriculum as part of Computing and PHSE, with e-safety teaching and learning embedded across the curriculum and central to a whole school approach
- Critical awareness of their own and other's online behaviour
- Effective strategies for staying safe online and making a positive contribution
- Key e-safety learning in response to current up to date guidance or concerns that arise
- Key e-safety messages reinforced as part of a planned programme of assemblies
- Pupils helped to understand the need for the pupil Acceptable Use Agreement and taught 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

### **PARENTS AND CARERS**

Parents and carers play an essential role in the education of their children and in the monitoring and regulation of the children's on-line behaviours.

The school will therefore seek to assist parents and carers and provide up to date guidance, support and advice through:

- curriculum activities
- letters and newsletters
- the school website,
- parent / carer information sessions
- high profile events / campaigns e.g. Safer Internet Day
- reference to relevant web sites / publications
- Twitter feed
- emails

## **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's E-Safety, Acceptable Use, and associated policies
- The E-Safety Champion 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 Champion 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:

- The Acceptable Use policy will be reviewed regularly
- All staff will have an individual user name and secure password for the system, Pupil users will be provided with an individual user name and password
- 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
- 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 Champion and MGL. Users are required to read and sign the Acceptable Use Policy
- Guests / children must have their memory sticks scanned by the office prior to usage in school to prevent viruses

## **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 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 / 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, particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website

## **MOBILE PHONES**

**See Mobile Phones & Devices Policy**

## **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, or try to use any other person's username and password.
- I will follow the school e-safety rules (SMART) at home and at school.
- I will immediately report anything that makes me feel uncomfortable when I see it online.
- I will be polite and responsible when I communicate online with others, both at home and at school. I understand that I will receive consequences if I make inappropriate comments about school, staff or other pupils.
- 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.
- If I need a mobile phone (only Y5 and Y6) I will switch it off at the school gate and give to my teacher as I enter the classroom.
- 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.

## **Pupil Acceptable Use Policy Agreement** **Reception, Y1 & Y2**

**This is how we stay safe:**

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 iPads, laptops and any other devices. I will use them sensibly.

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 will tell a teacher or adult if something pops up on the screen.

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

## Use of Digital Images and Video

The use of digital images and video play an important part in learning activities. Pupils and members of staff use digital devices as part of their learning and to record evidence in lessons and out of school.

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

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

Please complete and sign the permission form below.

### Permission Form

Parent / Carer Name: \_\_\_\_\_

Pupil Name: \_\_\_\_\_

Year Group & Teacher: \_\_\_\_\_

I agree to images and video being published on the school website, newsletter and school prospectus.

yes	no
yes	no

I agree to images and video being taken and used in the local press and on their website.

I agree that if I take images or video of school events, which include images of children other than my own, I will not publish them on social media or the internet.

Signed: \_\_\_\_\_

Date: \_\_\_\_\_

