# St. Paul's C of E (Aided) Primary School ('the School')

# Online Safety Policy

Policy date: Nov 2017

| Associated Policies | |
|---|---|
| **Title** | **Review Date** |
| Anti – Bullying | Sept 18 |
| Behaviour | Sept 17 |
| Computing | Pending |
| Data Handling | Pending |
| Mobile Technology | (merged) |
| PSHE | Jan 2019 |
| Safeguarding | July 2017 |
| Social Media | (merged) |
| Use of Images | (merged) |

| Appendices | |
|---|---|
| **Title** | **Page** |
| Acceptable Use Policy KS1 | 8 |
| Acceptable Use Policy KS2 | 9 |
| Online Safety Rules | 10 |
| Parent Carer Consent Form: Web Publication and Online Safety | 11 |
| Staff, Governor and Visitor Acceptable Use Agreement / Code of Conduct | 12 |

| |
|---|
| Member of Staff with Responsibility – Alexandra McLeod (OLS Coordinator) |

# St. Paul's C of E (Aided) Primary School ('the School')

# Online Safety Policy

Policy date: May 2017

## Aim

- To ensure all staff adopt safe practices in the use of the internet and in the teaching of internet use to children.
- To **educate** children to be responsible and informed internet users.
- To inform and support parents in keeping their children safe on the internet at home, on PCs or other internet-enabled devices, e.g. consoles, smartphones and tablets.

## Links and Reviewing

The Online Safety Policy is an integral part of the School's safeguarding responsibilities and relates to other policies including those for behaviour, safeguarding, mobile technology, acceptable use, anti-bullying, data handling, social media and the use of images.

The school has an Online Safety Committee who meet once a term. The committee members are:

**Deidre Malia** (AHT and DSL), **Hugh Hogan-Fleming** (ADHT, ICT Hardware SL, DDSL) **Alexandra McLeod** (Online Safety Coordinator), **Ian Simpson** (Governor), and **Dawn Moore** (ICT Technician),

- This Online Safety Policy has been written by the School, building on best practice and government guidance. It has been agreed by the Online Safety Committee and approved by Governors.
- The Online Safety Policy and its implementation will be reviewed annually.
- The Online Safety Policy was approved by the Governors on: [……. ]
- The Online Safety Policy covers the use of all technology which can access the school network and the internet or which facilitates electronic communication from school to beyond the bounds of the school site. This includes, but is not limited to, workstations, laptops, mobile phones, tablets and hand held games consoles used on the school site.
- The Online Safety Policy recognises that there are differences between the use of technology as a private individual and as a member of staff/ pupil.

## Teaching and learning

**Why Internet and digital communications are important**

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality computing, computer science and ICT experiences as part of their learning.

- The school will provide an age-appropriate online safety curriculum that teaches pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety.
- All communication between staff and pupils or families will take place using school equipment and/or school accounts.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- The school Internet access is provided by the RM contract, and includes appropriate filtering for staff and pupil users provided by RM Safety Net and managed and monitored by Dawn Moore and Hugh Hogan-Fleming.
- Pupils are taught what Internet use is acceptable and what is not and are given clear objectives for Internet use
- Pupils are educated in safe searching when using the Internet, and will be directed to safe and age appropriate digital resources.
- Pupils are shown how to publish and present information appropriately to a wider audience.
- Pupils are taught how to use online communication tools effectively and safely.
- Pupils will be advised not to give out personal details or information which may identify them or their location.
- Pupils will be taught how to evaluate Internet content
- The school uses the Rising Stars Scheme of Work, together with materials from Thinkuknow, to educate pupils in the safe use of social networking and the wider internet. The scheme is delivered termly and in longer units when appropriate.
- The school will seek to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Where possible, pupils are encouraged to verify the information they find online with other sources, e.g. books.
- Pupils will be taught how to report unpleasant Internet content e.g. using the CEOP Report Abuse icon, Hector Protector or by telling an adult.

## Managing Access and Security

The school will provide managed internet access to its staff and pupils in order to help pupils to learn how to assess and manage risk, to gain the knowledge and understanding to keep themselves safe when using the internet and to bridge the gap between school IT systems and the more open systems outside school.

**Information system security**

- The school will use a recognised internet service provider or regional broadband consortium. At present the School is using RM.
- The school will ensure that all internet access has age appropriate filtering provided by a recognised filtering system which is regularly checked to ensure that it is working, effective and reasonable.
- Access to school networks will be controlled by age appropriate passwords for children and strong person passwords for adults.
- Systems will be in place to ensure that internet use can be monitored and a log of any incidents will be kept to help to identify patterns of behaviour and to inform online safety policy.
- The security of School ICT systems will be reviewed regularly.
- The school will ensure that its networks have virus and anti-spam protection.
- All staff that manage filtering systems or monitor IT use will be supervised by SLT / OLS Committee and have clear procedures for reporting issues.

- The School will ensure that access to the internet via school equipment for anyone not employed by the school is filtered and monitored.
- Security strategies will be discussed with Classmaster, Surrey CC/Babcock4S

**E-mail**

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- The school may use class based email accounts. These are only used to send messages between classes in the school.
- Staff to pupil email communication must only take place via a school email address or from within a learning platform if introduced and will be monitored.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school will consider how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters or their current equivalents (e.g. 'memes' or viral content) is not permitted.

**Published content and the school web site**

- The contact details on the schools website, Twitter/Google+/ other social networking platforms or on a learning platform if introduced, should be the school address, web address, e-mail and telephone number.
- Staff or pupils' personal information will not be published, other than the names and responsibilities of staff.
- The Office Manager, Jane Shaw, and the Acting Deputy Headteacher, Hugh Hogan-Fleming, have responsibility for maintaining and reviewing the website. The Acting Headteacher, Deirdre Malia, has overall responsibility to ensure that content is accurate and appropriate.

**Use and Publishing of pupils' images and work**

- Written permission from parents or carers is obtained via a consent form on joining the school which may allow photographs of pupils to be published on the school Web site or in other publicity, unless objected to.
- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified e.g. via name tag or a book label. The school will look to seek to use group photographs rather than full-face photos of individual children where photos are published to social media.
- Pupils' full names will not be used on the school web site, particularly in association with photographs
- Parents are clearly informed of the school policy on image taking and publishing.
- Webcams are a useful tool for learning. They can allow an individual or class to interact over the internet with others and support links between pupils in different schools, countries and cultures.
- A webcam will only be used in appropriate circumstances such as a normal class setting.
- Both children and teachers will be made aware of when a webcam is in use.
- The School uses CCTV in some areas of school property as a security measure.
- Cameras will only be used in appropriate areas and there is clear signage indicating where it is in operation.
- Staff will supervise and maintain control over any photographing pupils do during in-school or off-site activities.

**Use of social media including the school learning platform**

Social media (e.g. Facebook, Twitter, Linkedin) is a broad term for any kind of online platform which enables people to directly interact with each other. However some games, for example Minecraft or World of Warcraft and video sharing platforms such as You Tube have social medial elements to them.

- The use of external social networking sites in school is not allowed by pupils, other than for supervised use in respect of the pupils' Twitter reporting account, or to demonstrate safe use in lessons.
- Within school, a limited range of social networking services may be provided if a learning platform is re-introduced. Their introduction would be staggered by age, allowing staff to introduce children to social networking in a safe and monitored environment.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils through parent Online Safety information and materials available via the website.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Use of video services such as Skype, Google Hangouts and Facetime will be monitored by staff if used during a lesson. Pupils must ask permission from a member of staff before making or answering a video call.
- Staff and pupils should ensure that their online activity, both in school and out takes into account the feelings of others and is appropriate for their situation as a member of the school community.

**Managing filtering**

- The school will work in partnership with Surrey County Council, and their online providers, to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the Online Safety Coordinator or staff responsible for filtering as above.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

**Managing emerging technologies**

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used during lessons or formal school time except as part of an educational activity. The sending of abusive or inappropriate text messages is forbidden.
- Mobile phone cameras will not be used for school purposes. Year groups are provided with cameras for this purpose.
- Children may use a class set of cameras for certain ICT work and during photography/newspaper clubs. Photos taken on these cameras will only be stored on school computers and used appropriately as per the Online Safety policy.
- As the use of iPads and other tablet devices becomes more widespread, they must be protected by a code lock where appropriate (for individual use) or kept in a locked cabinet and will be used appropriately to enhance lessons and teachers' work.
- Games machines including Playstation, Xbox and Wii have Internet access which may not include filtering. Children are educated about their safe use through Online Safety lessons and PSHE.
- Staff will use a school phone where contact with parents is required.
- The appropriate use of Learning Platforms is monitored and discussed as changes and additions in technology take place.

- External/guest devices connected to the school wireless network are subject to enhanced filtering using a separate proxy/port to the staff/pupil logins.

**Use of personal devices**

- Personal equipment may be used by staff and/or pupils to access the school IT systems provided their use complies with the Online Safety Policy and the relevant AUP.
- Staff must not store images of pupils or pupils' personal data on personal devices.
- The school cannot be held responsible for the loss or damage of any personal devices used in school or for school business.

**Protecting personal data**

- The School has a separate Data Handling Policy. It covers the use of biometrics in school, access to pupil and staff personal data on and off site, remote access to school systems.

# Policy Decisions

**Authorising Internet access**

- All staff (including teaching assistants, support staff, office staff, midday supervisors, student teachers, work experience trainees, ICT technicians and governors) must read and sign the 'Staff Acceptable Use Agreement ('AUA') /Code of Conduct for ICT/Computing' before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are granted access to school IT systems.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- At Key Stage 2, access to the internet will be with teacher permission with increasing levels of autonomy.
- Parents will be asked to sign and return a consent form for all children in every Key Stage to allow use of technology by their pupil.
- Any person not directly employed by the school will be asked to sign a Guest AUP before being given access to the internet via school equipment.

**Assessing risks**

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will not appear on a school computer. Neither the school nor SCC can accept liability for the material accessed, or any consequences of Internet access.
- The school audits ICT use and emergence of new technologies to establish if the Online Safety Policy is adequate and that the implementation of the Online Safety Policy is appropriate and effective.

**Handling Online Safety complaints**

- Complaints of Internet misuse will be dealt with by a senior member of staff and in accordance with the school behaviour policy.
- Any complaint about staff misuse must be referred to the headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.
- Complaints may be passed onto the LEA and the police if this is felt to be appropriate.

**Community use of the Internet**

- Members of the community and other organisations using the school internet connection will have signed a guest AUP so it is expected that their use will be in accordance with the School Online Safety Policy.

# Communication of the Policy

**To pupils**

- Appropriate elements of the Online Safety policy are shared with pupils
- Online Safety rules are posted in all school learning areas where the internet is accessed.
- Pupils are informed that network and Internet use will be monitored.
- The school uses the Surrey Online Safety scheme of work in order to teach children about relevant Online Safety issues and instil a set of safe behaviours when accessing the internet.
- Online Safety lessons are taught regularly throughout the school and links to the PSHE policy.
- Pupils need to agree to comply with the pupil AUP in order to gain access to the school IT systems and to the internet.
- Pupils will be reminded about the contents of the AUP as part of their online safety education.

**To Staff**

- All staff will be given the School Online Safety Policy and its importance explained.
- All staff must sign and agree to comply with the staff AUP in order to gain access to the school IT systems and to the internet.
- All staff will receive online safety training on an annual basis.
- Staff should be aware that Internet traffic can be monitored and traced.
- Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

**To Parents**

- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.
- Parents' and carers' attention will be drawn to the School Online Safety Policy in newsletters, the school brochure, on the school web site and on a learning platform if introduced.
- Parents and carers will from time to time be provided with additional information on Online Safety via the website, newsletters, parent mail or leaflet in order to reinforce messages of Online Safety outside of school.
- The School will host a regular Online Safety information session for parents and carers to attend.

Dated at front.
AMc/2017

Acceptable use of the school computers

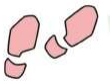
# Think then Click

**These Online Safety Rules help us to stay safe on the Internet in Reception, Year 1 and Year 2.**

**We can take care of the school computers.**

**We only use the internet when an adult is with us or has given us permission.**

**We can tell an adult if we see something on the internet that upsets us.**



**We will not tell people online personal things about us.**

**We can click on the buttons or links when we know what they do.**

**We can search the Internet with an adult.**

**We always ask if we get lost on the Internet.**

**We can send and open emails together with an adult.**

**We can write polite and friendly emails to people that we know.**

Acceptable use of the school computers

# Think then Click

**Online Safety Rules for Key Stage 2**

**These rules will help to keep everyone safe and help us to be fair to others.**

- We only use the School's computers for schoolwork and homework.
- We do not tell anyone our login and password.
- We only login to the School systems using our personal username and password.
- We only edit or delete our own files.
- We are aware that some websites and social networks have age restrictions which mean that we do not go on them.
- We only visit internet sites that are appropriate for our age.
- We only communicate with people we know, or that a responsible adult has approved.
- We send e-mails that are polite and friendly.
- We will not open an attachment, or download a file, unless we have been given permission by an adult.
- We never give out personal information such as our passwords, home address, or phone number.
- We never send a photograph or video, or give any other personal information that could be used to identify us, our family or our friends, unless a trusted adult has given permission.
- We tell a trusted adult if we see anything we are uncomfortable with or if we receive a message we do not like.
- We only e-mail people an adult has approved.
- We immediately close any webpage we are not sure about and speak to an adult.
- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We never arrange to meet anyone we don't know.
- We do not use Internet chat rooms.

## St. Paul's CE (Aided) Primary School

# Online Safety Rules

**All pupils use computer facilities, including internet access, as an essential part of learning, and as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the Online Safety Rules have been understood and agreed.**

| **Pupil's name:** | **Class:** |
|---|---|

**Pupil's Agreement**

- I have read and I understand the school Online Safety Rules.
- I will use the computer, network, mobile phones, Internet access and other new technologies in a responsible way at all times.
- I know that network and Internet access may be monitored.

| **Signed:** | **Date:** |
|---|---|

Please complete, sign and return to the school office together with the parent's consent form.

# St Paul's CE (Aided) Primary School

## Parent/Carer consent form: Web Publication and Online Safety

All pupils use computer facilities, including Internet access, as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign agreements to show that the Online Safety Rules have been understood and agreed.

**Parent / Carer name: ……**

**Pupil name: …….**

**Parent's Consent for Web Publication of Work and Photographs**

I agree that my son/daughter's work may be electronically published. I also agree that appropriate images and video that include my son/daughter may be published subject to the School rule that photographs will not be accompanied by pupil names.

**Parent/Guardian signature: ……..**

**Date: ……**

---

**Parent's consent - Online Safety Policy**

As the parent or legal guardian of the above pupil, I have read and understood the attached school Online Safety Rules and grant permission for my daughter or son to have access to use the Internet, School email system, learning platform and other ICT facilities at school.

I know that my daughter or son has signed an Online Safety Agreement form and that they have a copy of the School Online Safety rules. We have discussed this document and my daughter or son agrees to follow the Online Safety rules and to support the safe and responsible use of ICT at St Paul's School.

I accept that ultimately the School cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered service, restricted access email, employing appropriate teaching practice and teaching Online Safety skills to pupils.

I understand that the School can check my child's computer files, and the Internet sites they visit, and that if they have concerns about their Online Safety or e-behaviour that they will contact me.

I understand the School is not liable for any damages arising from my child's use of the Internet facilities.

I will support the School by promoting safe use of the Internet and digital technology at home and will inform the School if I have any concerns over my child's Online Safety.

**Parent/Guardian signature: ……..**

**Date: ……**

**Please complete, sign and return to the school office.**

# St Paul's C of E (Aided) Primary School

## Staff, Governor and Visitor - Acceptable Use Agreement / Code of Conduct

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents

- I will only use the school's ICT systems for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will use the approved RM Easymail system for school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
- I will not install any hardware or software without permission.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the School's Online Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- I will ensure that all my use of ICT devices, including computers, cameras, tablets and any other internet-enabled device, complies with the school Online Safety policy.

**User Signature**

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature …… Date ……

Full Name ……(printed)

Job title ……