All Saints C of E Infant School Tilford

E-Safety Policy

Co-ordinator responsible for this policy	Sharon Hedges
In consultation with Staff and Governors	
Date adopted	September 2018
Review date	September 2019

All Saints Infant School E-Safety Policy

E-safety is part of the school's safeguarding responsibilities. This policy relates to other policies including those for behaviour, safeguarding, anti-bullying, data handling and the use of images.

Using this policy

- The school has appointed an e-safety committee and e-safety coordinator (Sharon Hedges).
- Our e-safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior management and approved by governors.
- The e-safety policy was revised by: Sharon Hedges. All Governors will ensure they have read and understand the policy.
- The e-safety policy and its implementation will be reviewed annually. The next review is due on: September 2019
- The e-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 e-safety policy recognises that there are differences between the use of technology as a private individual and as a member of staff / pupil.

Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology.

Legislation and guidance

This policy is based on the Department's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying, and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

This policy also takes into account the National Curriculum computing programmes of study.

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.

- The school will use a recognised internet service provider or regional broadband consortium.

- 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.

- The school will ensure that its networks have virus and anti-spam and malware protection and such safety mechanisms are updated regularly.

- Access to school networks will be controlled by personal passwords.

- 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 e-safety policy.

- The security and monitoring of school IT systems will be reviewed regularly.

- All staff that manage filtering systems or monitor IT use will be supervised by senior management 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.

Internet Use

The school will provide an age-appropriate e-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.

Pupils will be taught to use technology safely and respectfully, keeping information private. They shall be taught not to give out personal details or information which may identify them or their location.

Pupils will be taught, through PSHE lessons, where to go for help and support when they have concerns about the content or contact on the internet or other online technologies.

E-mail

- Pupils and staff may only use approved e-mail accounts on the school IT systems.

- Staff to pupil email communication must only take place via a school email address or from within the learning platform.

- 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.

Published content eg school web site, school social media accounts

- The contact details will be the school address, email and telephone number. Staff or pupils' personal information will not be published.

- The head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupils' images and work

- Written permission will be obtained from parents or carers before photographs or names of pupils are published on the school web site or any school run social media as set out in Surrey Safeguarding Children Board Guidance on using images of children. http://www.surreyscb.org.uk/

Use of social media

- 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.

- Through IT lessons, children will be taught how to keep themselves safe online. Age appropriate resources and literature will be used.

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 e-safety policy and the relevant AUP.

- Staff must not store images of pupils or pupil 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.

- Personal devices of both staff, governors and visitors, such as mobile phones, tablets will be stored away in a locked container during the school day.

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 access

- All staff (including teaching assistants, support staff, office staff, midday supervisors, student teachers, work experience trainees, ICT technicians, governors and visitors) must read and sign the 'Staff AUP' before accessing the school IT systems.

- The school will maintain a current record of all staff and pupils who are granted access to school IT systems.

- Access to the internet will be by adult demonstration with supervised access to specific, approved on-line materials.

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 never appear on a school computer. Neither the school nor SCC can accept liability for the material accessed, or any consequences of internet access.

Handling e-safety complaints

- Complaints of internet misuse will be dealt according to the school behaviour policy.

- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

- Pupils and parents will be informed of consequences and sanctions for pupils misusing the internet and this will be in line with the schools' behaviour policy.

- Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with staff disciplinary procedures. The school will consider whether incidences which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Cyber-bullying

- To help prevent cyber-bullying, we will ensure that pupils understand what it is (in an age appropriate manner), and what to do if they become aware of it happening to them or others. We will ensure pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

- Complaints of cyber-bullying will be dealt with according to the school behaviour policy and parents informed.

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 e-safety policy.

Communication of the Policy

To pupils

- 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 e-safety education termly.

- Pupils considered at risk will be provided with appropriate and differentiated online safety education.

To staff

- All staff will be shown where to access the e-safety policy and its importance explained.

- All new staff will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

- The DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years.

- 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 e-safety training on an annual basis and receive regular updates regarding changes and guidance or emerging online safety concerns.

To parents

- Parents' and carers' attention will be drawn to the School e-safety Policy in newsletters, the school brochure and on the school web site. Links supporting guidance on keeping children safe online will be available on the school website.

- The school will raise parent awareness of internet safety by offering e-safety training annually through parent information evenings and providing lists of supporting organisations/resources on the school's website.

- If parents have concerns or queries in relation to online safety, these should be raised in the first instance with the Headteacher/DSL lead.

- Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

To Governors

- The governing body will co-ordinate regular meetings with appropriate staff to discuss online safety, monitor online safety log as provided by the designated safety lead (DSL).

- Governors will agree and adhere to the terms of acceptance of use of the school ICT systems and the internet.

Monitoring

The DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed annually by the e-safety coordinator. At every review, the policy will be shared with the governing board.