Shalford Infant School

ONLINE SAFETY POLICY
MARCH 2019

Policy Originator: Headteacher

Status:	Non-statutory	**Review Period:**	3 Years
Date:	March 2019	**Next review date:**	March 2022

Online 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 photography.**

Using this policy

- The school has an online safety committee and has appointed an online safety co-ordinator.
- Our Online 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 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.

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 protection.
- Access to school networks and staff shared area 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 online policy.
- The security 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.
- Physical monitoring of the internet by staff will ensure children are accessing appropriate content.
- 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 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, such as Parentmail.
- Pupils will be advised not to give out personal details or information which may identify them or their location.

E-mail

- Staff may only use approved e-mail accounts on the school IT systems.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

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.surreycc.gov.uk/?a=168635
- The school's photography policy details how and where all images may be published (with parental consent) and what information may accompany it.

Use of social media including the school learning platform

- The school will control access to social networking sites, and consider how to educate pupils in their safe use. This control may not mean blocking every site; it may mean monitoring and educating pupils in their use.
- Use of video services such as Skype, will be monitored by staff.
- Staff and pupils should use 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.
- When using social media on behalf of the school, it is important that staff do not bring the school into disrepute or harm its reputation through the use of unsuitable comments or images.
- Staff members can only use official school sites for communicating with parents and providing an audience for children's work.
- There must be a strong pedagogical or business reason for creating official school sites to communicate with parents or others. Staff must not create sites for trivial reasons which could expose the school to unwelcome publicity or cause reputational damage.
- Staff members must at all times act in the best interests of children and young people when creating, participating in or contributing content to social media sites.
- Permission to use social media must be authorised by the Headteacher.
- The following issues must be considered before creating a social media page:
  - How will this support pupil learning?
  - Who can communicate with us?
  - Is the communication open or closed?
  - How will images be used?
  - Do all children have permission to be featured on the school's social media sites?

How can users interact with the school's social media?

- Followers or friends of the school's social media sites must be adults. They should be parents of current pupils in the school. If other adults would like to become followers or friends, then permission must be granted by the Headteacher.

- Users who do not follow these guidelines may be suspended from accessing the school's social media pages.

Use of personal devices

- Personal equipment may not be used by staff and/or pupils to access the school IT systems.
- Staff must not store images of pupils or pupil personal data on personal devices.

Protecting personal data

- The school has a separate Data Protection Policy. It covers roles and responsibilities, remote access to school systems, and collection, storage, use and disposal of data.

Authorising 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 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.
- In Reception and Key Stage 1, access to the internet will be by adult demonstration with supervised access to specific, approved on-line materials.
- People not employed by the school must read and sign a Guest AUP before being given access to the internet via school equipment.
- Parents will be asked to sign and return a consent form to allow use of technology by their pupil.

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 online complaints

- Complaints of internet misuse will be dealt according to the school behaviour policy and/or data protection policy as appropriate.
- 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' behavior policy.

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 policy.

<u>Communication of the Policy</u>

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 online education

To staff

- All staff will be shown where to access the online 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 a bi-annual basis

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 and on the school web site.
- Parents will be offered online safety training regulary

Mobile Technology

General use of mobile phones

- Personally-owned devices may not be used during lessons or formal school time. They should be switched off (or silent) at all times.
- Personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- Personal devices are not permitted to be used in certain areas within the school site such as classrooms or toilets.
- Mobile devices will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with explicit consent from a member of staff and sanctioned by a senior member of the school.
- All adults must not use mobile devices in areas which children can access.
- Personal devices must not use 4G or 3G to access pornographic or other unsuitable materials on the school site.

Pupils' use of personal devices

- Children should not bring personal mobile phones or devices to school.

Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices for contacting pupils, young people or those connected with the family of the student.
- Mobile phones and personally-owned devices will be switched off or switched to 'silent' mode, Bluetooth communication should be 'hidden' or switched off and mobile phones or devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use school provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken as appropriate.
- Staff use of mobile phones during the school day will normally be limited to the lunch break and after school.
- Staff should ensure that their phones are protected with PIN/access codes in case of loss or theft.
- Mobile phones should be switched off and left in a safe place during lesson times. Staff should use mobile phones in designated areas. The designated area is the staff room. If a private call needs to be made then a request for a room can be made to the Senior Leadership Team or the school office.
- Staff should not connect mobile phones or other personal devices to the school's wireless network.

Appendix 1

ICT ACCEPTABLE USE POLICY/CODE OF CONDUCT JULY 2018

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 and visitors are aware of their responsibilities when using any form of ICT. All staff and visitors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the E-safety Co-ordinator.

- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes, or for uses deemed 'reasonable' by the Headteacher 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 understand that I am responsible for all activity carried out under my username.
- I will ensure that all electronic communications with parents and staff are compatible with my professional role.
- I will only use the approved, secure email system(s) for any 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 Headteacher or Governing Body.
- I will not install any hardware of software without the permission of the IT technician.
- 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/learning platform 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 the 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 report any incidents of concern regarding children's safety to the E-safety Co-ordinator, a Designated Safeguarding Lead or the Headteacher.
- I will ensure that electronic communications with pupils, parents and ex-pupils including email, IM and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will support the school's E-safety policy and help pupils to be safe and responsible in their use of ICT and related technologies. I will promote E-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I will ensure my school laptop (where applicable) has a secure password on it. I will use an encrypted USB pen that I will be supplied with. I will not use my own camera to take photos of children and I will not store/download any photos of children at my house on other devices or storage systems.

Appendix 2

Shalford Infant School

ICT Acceptable Use Policy for Visitors
MAY 2018

All visitors to Shalford Infant School must adhere to our Acceptable Use Policy for visitors. This policy covers email, the internet and mobile devices. **If you do not understand anything in this policy, please ask for clarification.**

- Mobile phones and other mobile devices are not allowed to be used on the school site.

- Photographs or videos of pupils must not be captured by parents or visitors on the school site, without the express permission of the Headteacher.

- If granted permission to capture images of pupils, the images must not be shared (i.e. on social media) if they clearly show any pupil other than your own child.

- Access to the school WiFi will not be granted to visitors. Requests to access the Guest WiFi will be considered based on visitor activities.

- Visitors who are granted access to our ICT network must not look at inappropriate materials such as pornography or extremist materials.

- If you witness anyone capturing images of a pupil at an inappropriate or not-permitted time, please report this to one of the Designated Safeguarding Leads immediately.