# Acceptable Use Policy

**'Every Child, Every Chance, Every Day'**

| | | | |
|---|---|---|---|
| **Reviewed By** | Susie Mew & Russell Hack | Policy Owner | May 2016 |
| **Ratified by** | Liam Peters | Governor | May 2016 |
| **NEXT REVIEW** | | | May 2018 |

Shirley Infant and Shirley Junior school are striving to create a community of pupils and staff who are competent, confident users of ICT and are knowledgeable about emerging technologies and able to incorporate these in their learning journeys. In order to achieve our aim, all ICT users must read and uphold the following standards:

- All users must take responsibility for their own use of new technologies, making sure they use technology safely, responsibly and legally.
- All users must be active participants in e-safety education, taking personal responsibility for their awareness of the opportunities and risks posed by new technologies. (See our e-Safety Policy and the pupil's e-safety rules.)
- Staff access to school systems must be through a unique user name and password, which must not be made available to any other staff member or pupil. The generic 'staff' user is available for students and non-regular supply.
- Users must ensure that unattended workstations are logged off or locked to ensure children cannot access sensitive data or the internet without supervision (closing laptop lids is sufficient for class computers).

**Internet**

- Staff must ensure that pupils are supervised at all times when using the internet.
- All internet activity should be appropriate to staff's professional activity or the students' education.
- Staff may use the internet facilities for non-business research or browsing outside of the school day (08:30-15:30) so long as said use does not interfere with those working and complies with the Acceptable Use Policy.
- Copyright, software licensing rules, laws of the land, property rights, privacy and the rights of others must be respected and adhered to at all times.
- The internet must not be used to access, display, store, transmit, distribute, edit or record inappropriate sites such as those containing pornographic, violent, racist, terrorist, discriminatory, criminal skills related, illegal drugs related or offensive material.
- Users will recognise materials that are inappropriate and, if deliberately accessing them, should expect to have their access removed.
- The internet must not be used to engage in any activity for personal gain.

- To ensure compliance with the Acceptable Use Policy for web browsing and email the school reserves the right to monitor and record user activity.
- All users have a responsibility to report any known misuses of technology, including the unacceptable behaviour of others. As soon as possible, concerns must be shared with the Head of School to investigate.

**Social Networks, Chat Rooms, Instant and Text Messaging**

- Staff must ensure pupils are taught safe and responsible behaviours whenever using ICT, by supporting and promoting the school's e-Safety policy.
- Staff must ensure that pupils are only given access to secure, age-appropriate chat rooms and social networks, which are approved within an educational context and moderated by a teacher, or approved adult.
- No online activity or applications accessed by users at any time may be used to bring the school, its members, or their own professional role into disrepute. Please also see the Social Networking Policy.

**Email**

- Access to school email should only be via the authorised user name and password, which must not be made available to any other staff member or pupil. Staff must not publish, electronically or otherwise, any school email address as a point of contact for non-education related activities.
- Staff may use personal emails.
- Attachments from unknown sources should be deleted immediately.
- As email can be forwarded or inadvertently sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media. Messages that contain abusive or objectionable language, that libel others, or that infringe the privacy rights of others are forbidden.
- Personal or otherwise sensitive data must not be transferred via email unless the security of the data whilst in transit can be assured.

**School Website**

- Only the designated staff members within the school may upload material to the school website and all material for the website must be monitored and approved by the persons responsible. The user name and password must not be given to any other members of staff or pupils.
- Images of pupils and staff should be classed as personal data under the terms of the Data Protection Act 1998. Therefore using such images for school publicity purposes, i.e. school website, will require the consent of either the individual concerned or in the case of pupils, their legal guardians.
- Recognisable photographs alongside full names, addresses, telephone numbers or email addresses of pupils must not be published on the school website. Home addresses and telephone numbers of school staff, parents and governors should not be published on the school website.

**DATA**

- Users must ensure that personal data (such as the data held on SIMS and the EYFSP) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.