Forest & Sandridge C.E. Primary School

Learn, achieve, have fun, succeed!

Headteacher: Mrs Anna Willcox
Deputy Headteacher: Mr Andrew Ind
School Business Manager: Miss Allison Moon

Forest & Sandridge C.E. Primary School
Sandridge Common
Melksham
Wiltshire
SN12 7QS
Tel/Fax: 01225 703394
Email: admin@forestsandridge.wilts.sch.uk
www.forestsandridge.co.uk

22nd November 2012

Dear Staff

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, well being and to support the professional work of staff and to enhance the schoolÕs management information and business administration systems. Internet access is an entitlement for students who show a responsible and mature approach to its use and we have a duty to provide students with quality internet access as part of their learning experience.

However, we also believe that staff have a responsibility to also ensure that they use the internet safely, following specific guidance rules for acceptable use of the internet whilst they are in school.

As part of our on-going commitment to improving the safety of our children when they are on-line, we are looking to ensure that all staff agree and adhere to these rules for acceptable internet use.

Acceptable Use - Staff

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

- Staff understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, PDAs, digital cameras, email and social media sites**.**

- School owned information systems must be used appropriately. Staff understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

- Staff understand that any hardware and software provided by the workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, staff will not

leave any information system unattended without first logging out or locking their login as appropriate.

- Staff will respect system security and they will not disclose any password or security information. They will use a ósstrongôpassword (A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system).

- Staff will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.

- Staff will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1988. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls) or accessed remotely. Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the school. Any images or videos of pupils will only be used as stated in the school image use policy and will always take into account parental consent.

- Staff will not keep professional documents which contain school-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are secured and encrypted. Staff will protect the devices in my care from unapproved access or theft.

- Staff will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.

- Staff will respect copyright and intellectual property rights.

- Staff have read and understood the school e-Safety policy (see below) which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.

  ósStaff use of ICT and information systems will always be compatible with their professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websitesô

- Staff will report all incidents of concern regarding childrenôs online safety to the Designated Child Protection Coordinator and/or the e-Safety Coordinator as soon as possible. Staff will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the e-Safety Coordinator or the designated lead for filtering as soon as possible.

- Staff will not attempt to bypass any filtering and/or security systems put in place by the school. If staff suspect a computer or system has been damaged or affected by a virus or other malware or if staff have lost any school related documents or files, then staff will report this to the ICT Support Provider/Team as soon as possible.

- Staff electronic communications with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number. Any pre-existing relationships which may compromise this will be discussed with the Senior Leadership team and, if deemed appropriate, approval will be given for it to continue.

- Staff use of ICT and information systems will always be compatible with their professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. Staff use of ICT will not interfere with their work duties and will be in accordance with the school AUP and the Law.

- Staff will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the County Council, into disrepute.

- Staff will promote e-Safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

- If staff have any queries or questions regarding safe and professional practise online either in school or off site, then staff will raise them with the e-Safety Coordinator or the Head Teacher.

- Staff understand that their use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

Please read through these rules for acceptable use and, as acceptance of these rules, please sign below and return the slip to Liz Wakeley as soon as possible.

Many thanks,

Anna Willcox
Headteacher

✂----------

Acceptable Use Policy

I confirm that I have read the staff rules for Acceptable Use of our Information Communication Technology and school systems and that I agree to adhere to them.

Signed _____

Name: _____

Position in school: _____

Date: _____