Staff ICT Acceptable Use Policy 2020

Witton-le-Wear Primary School

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.

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

2) School owned information systems must be used appropriately. I 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.

3) Mobile Phones. The school may have a separate mobile phone and tablet policy. (The distinction between a mobile phone and a tablet is becoming harder to define)

    a) Staff mobile phones will be stored in staff only areas during the school day and may only be used during breaks and out of teaching times.

    b) Staff mobile phones are allowed in school but are not allowed to be used in sensitive areas (EYFS, cloak rooms, toilets, when children are changing, swimming). Mobile phones should only be used for communication when not working with children. Mobile phones should not be visible to pupils unless their use is linked to learning, for instance as a stopwatch or to play music.

    c) Cameras on personal phones or tablets will not be used to take pictures of children in any circumstances.

    d) In the unlikely event of needing to contact a parent directly during trips or visits, a school mobile phone will be issued to the member of staff concerned.

4) I understand that any hardware and software provided by my school for staff use can only be used by members of staff and can only be used for school related work.

5) Personal use of school ICT systems and connectivity is only permitted with the consent of the headteacher.

6) To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

7) I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (A strong password has numbers, letters and symbols, with 10 or more characters, does not contain a dictionary word and is only used on one system).

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

9) Data Protection {*Schools should have a separate Data Protection Policy – some of the key guidance should be contained within the Staff AUP}*

   a) I 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 personal 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. {Secure means of transporting data are encrypted laptop/encrypted USB memory/encrypted HDD/approved cloud based system}

   b) If I choose to use a portable device (Phone, Tablet etc…) to collect my work e-mail I will ensure that the device is locked by a pin code or password and will be wiped when I dispose of the device.

   c) I will not transfer sensitive personal information from my school e-mail account (e.g. IEP's Safeguarding Reports, Medical Information) UNLESS the information is encrypted.

   d) I will not keep professional documents which contain school-related personal information (including images, files, videos etc.) on any personally owned devices (such as laptops, digital cameras, mobile phones) unless they are encrypted and will be wiped when I dispose of the device.

   e) Digital Images or videos of pupils will only be taken from the school premises using encrypted memory or an alternative secure transport method.

   f) I will not use unapproved cloud storage systems (Dropbox, icloud etc) for storing personal data of staff or pupils.

10) I 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.

11) I will respect copyright and intellectual property rights.

12) Social Media. Some schools may have a separate social media policy.

   a) I have read and understood the school e-Safety policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media.

   b) I will not communicate with pupils or ex-pupils using social media without the express permission of the Headteacher. *{Some schools may use social media to communicate directly with pupils, in this instance staff should use a social media account that is purely used for work purposes. They should complete a risk assessment to ensure that both staff and pupils are protected.}*

   c) My 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. *This would include any relatives of current pupils that are my "friends" on a social media site.*

   d) My use of ICT and information systems will always be compatible with my 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. My use of ICT will not interfere with my work duties and will be in accordance with the school AUP and the Law.

   e) I 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. This would include any comment made, even in the belief that it is private on social media.

13) I will report all incidents of concern regarding children's online safety to the Designated Child Protection Coordinator (Mr Stephenson) and/or the e-Safety Coordinator (Mrs Redfern) as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to Mrs Redfern, the e-Safety Coordinator or Mr Stephenson the designated lead for filtering as soon as possible.

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

15) I 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.

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

17) I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood and agree to comply with the Staff ICT Acceptable Use Policy.

Signed: …….…….. Print Name: ……..…… Date: ……..

Accepted by: …… Print Name: ……