Dore Primary School

Acceptable Use Policy

2017

Version	2.0
Author	M.Smith & J. Fletcher
Date Approved by Governing Body	February 2018
Review Date	February 2019

Dore Primary School Acceptable Use Policy

For staff, governors, volunteers & visitors to site.

September 2017
Updated December 2017

Staff ICT Acceptable Use Policy 2017

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.

School Systems

- 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, PDAs, digital cameras, email and social media sites**.**
- 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.
- I understand that any hardware and software provided by my 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, I will not leave any information system unattended without first logging out or locking my login as appropriate.
- I will respect system security and I will not disclose any password or security information. I will use a 'strong' password.
- I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.
- 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 or accessed remotely. Any **sensitive data** should be accessed in school or via Remote Access wherever possible and not stored locally on any devices.
- I will not keep documents which contain school-related information (including images, files, videos etc.) on any personal devices. I will protect the devices in my care from unapproved access or theft.
- 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.
- I will respect copyright and intellectual property rights.
- I have read and understood the school Online Safety policy 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.
- I will report all incidents of concern regarding children's online safety to the Designated Safeguarding Lead (Jason Fletcher) and the Online Safety Coordinator (Matthew Smith) as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the Online Safety Coordinator as soon as possible.
- I will not attempt to bypass any filtering and/or security systems put in place by the school unless I have permission. 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 Online Safety Coordinator as soon as possible

- 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. Exception to this is when away on school trips and an emergency call is needed to be made. If time allows, outgoing numbers should be blocked in these circumstances.
- 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 City Council, into disrepute.
- I will promote Online 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 I have any queries or questions regarding safe and professional practice online either in school or off site, then I will raise them with the Online Safety Coordinator or the Head Teacher.
- 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.

Social Media

Please read the school staff Social Media Policy

Mobile Phones

Staff are allowed to have mobile phones on site. However the following guidance must be followed to ensure the safety of children in our care and also safeguard yourself.

- Mobile phones must be kept out of site when children are present.
- They can be used in the staff room and in classrooms when children are not present (e.g. breaktimes, lunchtimes and after school).
- A reminder that our Online Safety Policy states that no personal devices should be used for the recording of video or taking images of children.
- School Trips - Mobile phones can be used to contact parents in an emergency. Where possible this should be done after blocking your outgoing number.