



THE HERMITAGE and THE OAKTREE SCHOOLS

School Staff ICT Acceptable Use Policy

Person responsible:	Computing Leader and Behaviour & Welfare Leader
Date Adopted:	July 2013
Date of last review:	Summer Term 2023
Date of next review	Summer Term 2024

Policy Links

ICT Policy

Online Safety Policy

Social Media Policy

Visual Images Policy

Password Policy

Rationale

This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of Information Communication Technology (ICT). This policy is not intended to unduly limit the ways in which members of staff teach or use ICT, but aims to ensure that the school and all members of staff comply with the appropriate legal responsibilities, that the reputation of the school is maintained and that the safety of all users is ensured.

To ensure that members of staff are fully aware of their professional responsibilities when using ICT and the school systems, they are asked to sign a register to confirm they have read and agree to follow this Acceptable Use Policy (AUP).

As a professional organisation with responsibility for children's safeguarding it is important that all staff:

- Use the school's computer system in a professional, lawful, and ethical manner.
- Take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft.

Any concerns or clarification regarding this policy should be discussed with the Executive Headteacher or member of the Senior Leadership Team.

Members of staff are entitled to seek their own legal advice on this matter before signing to say they will comply with the policy.

Code of Conduct

NB: The following list 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.

- I understand that ICT includes a wide range of systems, networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, digital cameras, email, social networking. I understand that it 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.
- My use of ICT will not interfere with my work duties and will be in accordance with all relevant school policies and the law.
- I will comply with the ICT system security and not disclose any passwords provided to me by school or other related authorities. There may be exceptions to this under certain circumstances – please see Password Policy (Audit/Monitoring/Reporting) for further guidelines.
- 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 use a 'strong' password (see Password Policy).
- I will only use the school's email/ internet/ learning platform and any related technologies for professional purposes, or for uses deemed 'reasonable' by the Executive Headteacher or Local Governing Committee.
- I will only use the approved, secure email system for school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and used appropriately, whether in school, taken off the premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Executive Headteacher or Local Governing Committee.
- Any data which is being removed from the school site must be saved on an encrypted laptop or encrypted memory stick provided by the school. Any data being removed by email must be secured/encrypted appropriately, if it contains any school-related sensitive or personal information.
- I will do my best to 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 not attempt to install any hardware or software without permission from the Executive Headteacher and Computing Leader.

- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I will respect copyright and intellectual property rights.
- 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/carers and Executive Headteacher.
- I will ensure that my online activity, both in school and outside school is in accordance with the school's Social Media Policy, and that it will not bring my professional role into disrepute.
- I will ensure that all electronic communications with parents/carers, pupils, staff and other professionals, including email, IM and social networking, are compatible with my professional role and that messages cannot be misunderstood and misinterpreted.
- My electronic communications with parents/carers, pupils, staff 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 Executive Headteacher.
- I will support the school's Online Safety Policy and help pupils to be safe and responsible in their use of ICT and related technologies. I will promote Online Safety with the students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I will report all incidents of concern regarding children's online safety to one of the Designated Safeguarding Leads as soon as possible.
- I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to one of the Designated Safeguarding Leads as soon as possible.
- I have read and understood the school ICT Policy, Online Safety Policy and Social Media Policy which cover 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.
- 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 Online Safety Leader or the Executive Headteacher.
- I understand that my use of the school information systems, the internet and email may be monitored and recorded to ensure policy compliance.
- I understand that sanctions for disregarding any of the above will be in line with the school's disciplinary procedures and that serious infringement may be referred to the police.