

## Staff ICT Acceptable Use Policy

As a professional organisation with responsibility for safeguarding it is important that 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 technology, they are asked to read and sign this Acceptable Use Policy. This is not an exhaustive list; all members of staff are reminded that IT use should be consistent with the school ethos, school policies, national/local guidance and expectations, and the Law.

1. I understand that Information Systems and IT include networks, data and data storage, online and offline communication technologies and access devices. Examples include laptops, mobile phones, tablets, digital cameras, e-mail 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. 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 protect the devices in my care from unapproved access or theft.
4. 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 8 or more characters, does not contain a dictionary word and is only used on one system and is changed regularly.
5. I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.
6. I will ensure that any personal data of pupils, staff or parents / carers is kept in accordance with the General Data Protection Regulation.
  - 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 data containing personally identifiable information which is being removed from the school site (such as via e-mail or on memory sticks or CDs) will be encrypted.
  - 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 recorded within school's MIS.
7. I will not keep professional documents which contain school-related sensitive or personal information, including images, files, videos and e-mails, on any personal devices, such as laptops, digital cameras, and mobile phones.
8. If school e-mails are accessed on a phone or tablet, then the device must be password / PIN protected. When not in use, the device must be locked.
9. If a data breach occurs, I will immediately report it to the Data Protection Officer. Any data (digital or hard copy) that has been mislaid, lost or sent to the wrong address needs to be reported. This includes:
  - loss or theft of memory sticks, portable hard disk drives, laptops and tablets.
  - e-mails, text messages, app notifications or letters sent to the wrong address.
  - loss or theft of phone or other device with school e-mails enabled.
10. I will not store any personal information on the school computer system including any school laptop or similar device issued to members of staff that is unrelated to school activities, such as personal photographs, files or financial information.
11. I will respect copyright and intellectual property rights.
12. I have read and understood the school online safety policy which covers the requirements for safe IT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces. These documents can be located on the Staff Shared area.
13. I will immediately report any illegal, inappropriate or harmful material or incidents I become aware of, to the Designated Safeguarding Lead 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 IT Support as soon as possible.
15. My electronic communications with current or past pupils, parents/carers and other professionals will take place within clear and explicit professional boundaries and will be transparent and open to scrutiny at all times.
  - All communication will take place via school approved communication channels such as a school provided e-mail address or telephone number, and not via personal devices or communication channels, such as personal e-mail, social networking or mobile phones.
  - Any pre-existing relationships or situations that may compromise this will be discussed with the Designated Safeguarding Lead and / or Headteacher / Head of School.
16. I will ensure that my online reputation and use of IT and information systems are compatible with my professional role, whether using school or personal systems. This includes the use of e-mail, text, social media, social networking, gaming and any other devices or websites.
  - I will take appropriate steps to protect myself online as outlined in the Online Safety policy and will ensure that my use of IT and the internet will not undermine my professional role, interfere with my work duties and will be in accordance with the school code of conduct / behaviour policy and the Law.
17. I will not create, transmit, display, publish or forward any material online 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 trust, into disrepute.
18. 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.
19. 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 Designated Safeguarding Lead and / or the Headteacher / Head of School.
20. I understand that my use of the school information systems, including any devices provided by the school, school internet and school e-mail may be monitored and recorded to ensure the safety of children and staff and to ensure policy compliance. This monitoring will be proportionate and will take place in accordance with data protection, privacy and human rights legislation.
21. I understand that 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 policy compliance. Where it believes unauthorised and / or inappropriate use, or unacceptable or inappropriate behaviour may be taking place, the school may invoke its disciplinary procedures. If the school suspects criminal offences have occurred, the matter will be brought to the attention of the relevant law enforcement organisation, as directed by leadership.

<b>I have read, understood and agree to comply with <b>xxxxx School</b> Staff ICT Acceptable Use Policy.</b>	
Member of Staff Name:	
Member of Staff Signature:	
Date:	
Accepted by:	
Date:	