



Acceptable Use Agreement

REVIEWED SUMMER 2016

'Green Lane – a Big School with a Big Heart'



GREEN LANE PRIMARY ACADEMY



ICT Acceptable Use Agreement

'New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools which open up new opportunities for everyone, enhancing teaching and learning across the curriculum. All users should have an entitlement to safe internet access at all times.'

SWGfL

Green Lane Primary Academy is a professional organisation with responsibility for children's safeguarding. Therefore, it is important that our 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 academy'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 (ICT) and the school systems, they are asked to read and sign our Acceptable Use Agreement.

The Acceptable Use Agreement is part of our e-Safety Policy and sits alongside other, more comprehensive, guidance, governing staff use of social networking sites, mobile phones and email.

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.

- 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, tablet computers, digital cameras, e-mail 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 or software provided by school for staff use can only be used by members of staff and only for educational use. Use of school equipment or internet access for business, profit, advertising or political purposes is strictly forbidden.
- 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 not disclose my password or log anyone into my account, nor will I try to access someone else's personal files. I will use a 'strong' password (a strong password has numbers, letters and symbols, 8 or more characters, does not contain a dictionary word and is only used on one system).
- I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the Leadership Team.

- I will ensure that any personal data of pupils, staff or parents 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 stored privately and securely. Any data removed from the school site must only be done so via school laptops or an encrypted (password protected) memory stick.
- I will not keep professional documents which contain school-related sensitive or personal information on any personal computers or devices, unless they are secured and encrypted. I will take all reasonable measures to protect school devices in my care from unapproved access or theft. At school, I will ensure my laptop is stored securely and not left on view in my classroom overnight.
- I will ensure that when I capture or publish images and videos of others I do so with permission (Pupil Profiles must be checked). I will never use my personal equipment to record these images. Photographs / videos of children should be stored on the network, not on laptops, and must never be taken off the school site. Wherever these images are published, it will not be possible to identify by name, or other personal information, those who are featured. Written permission must be sought from parents / guardians if photographs are to appear in newspapers.
- I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, music, files or financial information.
- I will respect copyright and intellectual property rights. Where work is protected by copyright, I will not download or distribute copies (including music and videos) without permission.
- 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 websites and the supervision of pupils within the classroom and other working spaces.
- My electronic communications with pupils, parents 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 Leadership Team. I will not access personal email accounts on school ICT systems or use my school email for personal messages.
- My use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. (In the case of teachers, this will be in line with the Teacher Professional Standards). 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.

For further guidance, see attached rules for staff use of social networking sites, mobile phones & e-mail.

- 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 academy, or the Council, into disrepute.

- 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.
- I will report all incidents of concern regarding children's online safety to the Designated Child Protection Officers (Mrs J. Lucas / Mrs Walsh / Mrs L. Tate) and the e-Safety Leader (Mr D. Carr) immediately.
- I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the e-Safety Leader.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes. I will only use the encrypted memory stick provided by the academy and always scan it for viruses first. I will not attempt to bypass any filtering or security systems. If I suspect a computer or system has been damaged or affected by a virus or if I have lost any school related documents or files, then I will report this to the ICT TLR or Leadership Team as soon as possible.
- 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 Leader or Leadership Team.
- I understand that my use of the information systems, internet and email may be monitored and recorded to ensure policy compliance.

The School will exercise its right, via the use of forensic software, 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 academy'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 academy will invoke its disciplinary procedure. If the academy 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.



GREEN LANE PRIMARY ACADEMY



ICT ACCEPTABLE USE AGREEMENT

I have read, understood and agree to comply with the ICT Acceptable Use Agreement.

Name:

Signed:

Date: