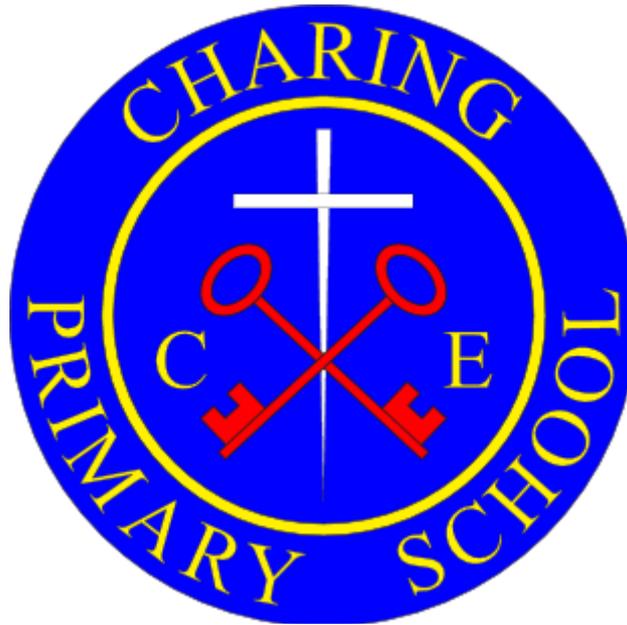


*...those who hope in the LORD will renew their strength.
They will soar on wings like eagles; they will run and not grow weary, they will
walk and not be faint.' Isaiah 40:31*

connect | nurture | aspire | learn | excel | hope



Charing Church of England Primary School

ICT Acceptable Use Policy

Document Information	Date/source of Policy	Responsibility
Date of review	September 2019	EHT/SLT
Date of new review	September 2020	EHT/SLT

Our Vision - *As an inclusive community built on friendship and love, Christian values inspire us through faith in God and hope for the future. Everyone is empowered to recognise their God-given potential and to become lifelong learners. We work together to ensure we achieve our aspirations and encourage independence.*

Love Friendship Kindness Truth Hope

ICT ACCEPTABLE USE POLICY

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.

Please read and sign where indicated:

- * 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 with prior permission, 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 (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). I will follow the KLZ password policy in respect of password changes.
- * I will not attempt to install any purchase or downloaded software, including browser toolbars, or hardware without permission.
- * I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 2018. 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 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. 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.
- * I will not use my own personal devices i.e.; laptop, iPad, camera in school for any reason and understand that if I do, this could result in formal action being taken.
- * I will not keep professional documents which contain school related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones) unless they are secured and encrypted. A secured encrypted pen drive is provided for this. KLZ can be used to store plans etc...
- * 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. This includes desktops and screen savers.
- * I will respect copyright and intellectual property rights. Further information on what is copyright protected can be found at this website address: <http://www.copyrightandschools.org/>
- * 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 (Please refer to the e-Safety policy). I will report all incidents of concern regarding children's online safety to the Designated Safeguarding Lead and/or the e-Safety Coordinator as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches and unsuitable websites to the Head of School or deputy Head of School as soon as possible.
- * 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 BCTEC or their appointed technician as soon as possible for technical help. ICT technical help can be reported via the BCTEC helpdesk.
- * 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.
- * 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.
- * I understand that all friends, with current or past connection to the school, on social network sites (including dating) must be declared to the Head of School to ensure transparency. No mention of working life should be made in anyway. All privacy settings should be set to the highest level to ensure that they not seen by the wider community. No friends under the age of 13.
- * 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 Aquila, 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 and publish.
- * 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 Head of School.
- * I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- * As part of safeguarding in school I understand that it is my responsibility to bring to the attention of the Head of School any inappropriate activities online or other by my partner or family that is not considered within the AUP policy and the law.
- * I understand that I should inform the Head of School if I use an 'alias' on any social networking site or any other internet site.
- * If I use my work email address for anything other than to carry out my job role, I will need to inform the Head of School.
- * When I am photocopying text or images from either an original hardcopy book, from an original hardcopy magazine, journal or periodical, an entire cutting from an original hardcopy newspaper I will have to check that the correct licenses are in place in order for me to do so.

- * When using music in a lesson, in collective worship/assemblies or for extra-curricular use, I must ensure that I am aware of the different licenses that are in place for the different scenarios and that I know what the licenses do and do not cover

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 strong unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

*** I have seen this document.**

Signed: Print Name:
Dated:.....

*** I agree and accept this document.**

Signed: Print Name:
..... Dated:.....

*** Please sign where indicated and return this form to the SBM**

Comments if not accepted:

.....
.....
.....
.....
.....