CUDHAM CHURCH of ENGLAND PRIMARY SCHOOL

AQUINAS Church of England Education Trust "Life - Transforming – Learning"

Policy Title:	**E Safety**
LT Responsibility:	Headteacher
Review Body:	Trust Improvement Partner
Date:	February 2020
Review:	February 2021

Together we aim believe and achieve

At Cudham CE Primary School we want the very best for the children in our care so that they flourish in our Christian community and realise their potential. We strive to provide an enriching environment where each child will be happy, thrive and succeed.

We recognise that our pupils bring with them a wide variety of behaviours influenced by life experiences outside school. We aim to respond to each case professionally, objectively and compassionately. We are sensitive when working with children and families with specific needs and experiences and we continuously seek ways to promote successful partnerships. The basis of differentiation will vary dependant on the needs of each case but we will take into account the views of parents and families, colleagues and external agencies together with any Statement of Special Educational Need or Education, Health and Care Plan. We will also ensure compliance with the trust's Equality Policy taking into account pupils with protected characteristics and making reasonable adjustments for pupils with a disability within the meaning of the Equality Act 2010. Both the school and trust respects the Public Sector Equality Duty (PSED) that requires public bodies to have due regard to the need to eliminate discrimination, advance equality of opportunity and foster good relations between different people when carrying out their activities. By following the trust's Equality Policy, the school seeks to eliminate unlawful discrimination, harassment and victimisation and other conduct prohibited by such legislation.

This policy should be read in conjunction with the Trust's Equality Policy.
https://www.aquinastrust.org/

Context

There are many computers available for use by pupils and the majority of these have access to the internet through the school network. Pupils have access to a user name and password.

The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that:

- Pupils can only access data to which they have right of access.
- No pupil should be able to access another's files without permission.
- Access to personal data is securely controlled in line with the school's data policy.

CUDHAM CHURCH of ENGLAND PRIMARY SCHOOL

- Logs are maintained of access by pupils and of their actions while users of the system.

The internet provides children and young people with a wealth of opportunities for their education, entertainment and communication. But there are also risks of harm through the deliberate behaviour of others online, and through exposure to inappropriate content. St George's Bickley Church of England Primary School has procedures in place to safeguard all children from unlawful, sexual or otherwise potentially harmful content on the internet. Information on internet safety and the importance of monitoring internet use at home is made available to all parents annually.

At Cudham Church of England Primary School, all our systems are closely monitored.

Objectives and targets
The objective of this policy is to develop an appropriate code of practice for use of ICT by pupils at Cudham Church of England Primary School.

Action plan
All pupils are expected to abide by the teachers' instructions and rules.

Rights of access – pupils
A safe and secure username/password system is essential and will apply to all school ICT systems, including email and virtual learning environment (VLE).

All passwords are generated by the network manager/ICT technical support staff and are unique to each class. Passwords can only be reset by the user or by the ICT technical team. All pupils will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the network manager and these will be reviewed, at least annually. The 'master/administrator' passwords for the school ICT system used by the network manager/ICT technical support team are also available to the head teacher or other nominated senior leaders. In the event of a serious security incident, the police may request, and will be allowed access to, passwords used for encryption.

ICT code of practice – pupils
The facilities are provided to support and enhance curriculum-related activities. Each class will be issued with his/her own username and password, which must be kept confidential. Pupils must remember to log off when they have finished using the computer. It is good practice to change passwords regularly.

- The pupil's school email address must always be used for all school-related activity.
- Personal emails must not be used for any school-based activity.
- The use of another person's user name and password, abusive language, sending abusive messages and changing computer settings are all serious offences.
- Pupils must not copy, alter, print or change another pupil's work in any shape or form without the person's prior knowledge and consent. Please note that copyright regulations apply to electronic publications as they do to paper.
- Pupils must use the internet and printing facilities only to support their school work.
- Pupils should be aware that information on the internet may not always be reliable and sources should be checked. Also websites are used for advertising material, which may influence the contents.

CUDHAM CHURCH of ENGLAND PRIMARY SCHOOL

Emails are not confidential and do go astray. Therefore we must guard against any abuse which will bring the school into disrepute.

- Pupils must not disclose to anyone on the internet their home address, telephone number, the name of the school or a photograph of themselves unless specific permission is given from a member of staff. Nor should they ever arrange to meet anyone unless this is part of a school project approved by their teacher.
- Pupils must never pretend to be anything or anyone that they are not and must be aware that the posting of anonymous messages is forbidden.
- Pupils must not engage with internet chatrooms.
- If a pupil sees something which makes her/him feel worried or uncomfortable, she/he should report it immediately to a member of staff and never respond to bullying, suggestive or unpleasant emails or blog entries.
- Pupils must not send abusive email, chain email, excessive quantities or excessive sized emails. Nor must they use email to send or encourage material that is pornographic, illegal, offensive or invades another's privacy.

Pupils must not vandalise the system by:

- Physical damage.
- Changing configuration or cabling unless specifically directed by a member of staff.
- Hacking of the school or external systems.
- Changing the contents of the hard disks.
- Downloading or installing software onto the network, unless written as part of an approved school computer project and with the teacher's permission.
- Bringing food and drink into computer areas or in the vicinity of classroom computers because spillages can cause serious damage to electronic equipment.

Serious offences and other inappropriate use of ICT facilities will result in the following sanctions:

- An immediate ban from the network pending investigation.

- A letter home informing parents of incorrect ICT use and a minimum ban of two weeks from the internet facilities.
- Subsequent offences will lead to a four to eight week ban and/or an exclusion of three days from school.
- More serious or long term abuse will lead to a total network ban and possible exclusion from school.

Misuse of computer systems by pupils

Internet and email

Please note that in the case of misuse of internet and email facilities the following action will be taken:

First offence – the pupil will be reported to the network manager and will have access to the internet and email withdrawn for two weeks. Parents will be informed. The pupil will still have access to intranet and basic application software.

CUDHAM CHURCH of ENGLAND PRIMARY SCHOOL

Second offence – procedure as above but with a four week ban and a formal letter sent home to parents.

Third offence – parents will be invited to a formal meeting with the e-safety member of the senior leadership team, to discuss the way forward and sanctions.

Pupils who use other pupils' accounts and access restricted file areas
These are considered to be serious offences. The network manager will record the offence and will immediately inform the year tutor of the situation. Suspension of a pupil's access to all ICT facilities will take place after the year tutor has informed the appropriate staff.

The length of the ban may vary according to circumstances but it is likely to be for at least four weeks. To restore access, a note is required from the head teacher.

Damage to hardware

If a pupil damages hardware, the network manager will contact the main office staff. A letter will be sent to parents. The pupil will be charged for the damage.

Under exceptional circumstances, such as abuse which may be detrimental to the school network, the network manager may disable a pupil's account with immediate effect.

Monitoring and evaluation
The policy will be monitored and evaluated regularly taking into account any incidents which occur or technological developments which might need a change in the policy.

Reviewing
The efficacy of the policy will be discussed annually as part of the rolling programme of reviews.

DATA PROTECTION
Cudham CE Primary School [The Academy] processes personal data, some of which will be sensitive personal data, in accordance with the data protection principles embodied in the General Data Protection Regulations (GDPR) and the Data Protection Act 2018. The Academy complies with the requirements of the data protection legislation as detailed in the Trust Data Protection Policy.

All staff are aware of the principles of data protection and will not process personal data unless necessary. The Academy safeguards the personal data it collects through the operation of the Trust's data protection policy and processes and the IT policy. In addition, the Academy has taken steps to ensure that all its contracts that process data have the GDPR compliant provisions.