CUDDINGTON AND DINTON CHURCH OF ENGLAND SCHOOL
POLICIES AND PROCEDURES

E Safety

Date Reviewed September 2018

Date adopted by Governing Body _____

Date for next review by Governing Body September 2019

For clarity, the E-safety policy uses the following terms unless otherwise stated:

Users - refers to staff, Governors, school/parent volunteers, pupils and any other person working in or on behalf of the school, including contractors.

Parents – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.

School – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.

Wider school community – pupils, all staff, governing body, parents, visitors

Safeguarding is a matter taken very seriously at Cuddington and Dinton Cof E School and we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as E-safety is an area that is constantly evolving and as such this policy will be reviewed on a two year cycle or in response to an E-safety incident.
The primary purpose of this policy is twofold:
To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the pupil or liability to the school.

Roles & Responsibilities

1. Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy at least every two years and in response to any E-safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure E-safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.
- The Teaching & Learning Committee will oversee the implementation and review of the policy ensuring they:
    - Keep up to date with emerging risks and threats through technology use.
    - Receive regular updates from the Head and Assistant Head in regards to training, identified risks and any incidents.
- Be vigilant in their personal use of social media and be aware of how this reflects on the school, upholding the school values and therefore not undermining them.

2. Head Teacher

Reporting to the governing body, the Head has an overall responsibility for E-safety within our school and across both sites. The day-to-day management of this will be delegated to all members of staff.
The Head Teacher will ensure that:

• E-safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. pupils, all staff, senior leadership team and governing body, parents.
• All E-safety incidents are dealt with promptly and appropriately.
• Staff keep up to date with the latest risks to children whilst using technology; familiarise themselves with the latest research and available resources for school and home use.
• Review this policy regularly and bring any matters to the attention of the staff and governors.
• Staff engage with parents and the school community on E-safety matters at school and/or at home.
• Staff liaise with the local authority, IT technical support and other agencies as required.
• Staff retain responsibility for reporting e-safety concerns and incidents; ensure staff know what to report and to record appropriately.
• Any technical E-safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or ICT Technical Support.
• Staff make themselves aware of any reporting function with technical E-safety measures, i.e. internet filtering reporting function; to decide on what reports may be appropriate for viewing.
• All details within this policy are understood by all Staff (teaching and non-teaching). If anything is not understood it should be brought to the attention of the Head or Assistant Head.
• Any E-safety incident is reported to either the Head or Assistant Head or a Designated Safeguarding Lead in their absence.

3. ICT Technical Support Staff
Technical support staff are responsible for ensuring that:
• The IT technical infrastructure is secure; this will include at a minimum that Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
• Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
• Any E-safety technical solutions such as Internet filtering are operating correctly.
• Filtering levels are applied appropriately and in accordance with Bucks CC filtering provision.

4. All Staff
In accordance with the Staff Code of Practice and Safeguarding Policy, staff must ensure that:
• They retain responsibility for reporting e-safety concerns and incidents to the Head or Assistant Head.
• Model, remind pupils and enforce safe and appropriate use of the internet.
• They are vigilant and professional in their use of school hardware and social media, reflecting the school values and therefore not undermining them.

5. All Pupils
All pupils have the opportunity to use a range of ICT equipment and are expected to treat it with the utmost of respect and in accordance to the Pupil Code of Practice;

deviation or misuse of ICT equipment or services will be dealt with in accordance with the Behaviour Policy.

E-safety is embedded into our curriculum; pupils will be given the appropriate advice and guidance by staff. Similarly all pupils will be fully aware how they can report areas of concern whilst at school or outside of school.

6. Parents and Carers
Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through parent workshops, school newsletters and the weekly update emails, the school will keep parents up to date with new and emerging E-safety risks, and will involve parents in strategies to ensure that pupils are empowered.

Parents must also understand the school needs have to rules in place to ensure that their child can be properly safeguarded. As such parents will sign the Pupil Code of Practice document before any access can be granted to school ICT equipment or services.

We would expect that parents would inform us if their child has been exposed to inappropriate material (games, messaging etc)

7. The Teaching, Learning, Safeguarding and Assessment Committee
The Teaching, Learning, Safeguarding and Assessment Committee is responsible for e-safety monitoring and change, meeting on a termly basis and will therefore:
• advise on changes to the E-safety policy.
• establish the effectiveness (or not) of E-safety training and awareness in the school.
• recommend further initiatives for E-safety training and awareness at the school.

The Technology
Cuddington and Dinton CE School uses a range of devices including PCs, iMacs, laptops, iPads and interactive screens. In order to safeguard the pupils and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering – we use Bucks County Council (BCC) filtering software, Netsweeper Cloud Manager, to prevent unauthorised access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The Head Teacher and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to each other's and the Governing Body's attention.

Email Filtering – we use BCC software that prevents any infected email to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message. School and Staff emails are managed through the BCC Outlook provision; pupils do not have access to any external email service.

Encryption – All school devices that hold personal data (as defined by the Data Protection Act 1998) are encrypted. All documentation and dat from external agencies is accessed via a secure portal and should not be emailed between staff. Internal assessment data is only stored and processed on school devices.

Passwords – all staff and pupils will be able to access any device without a unique username and password. An adult will always be supervising any child on an electronic device capable of accessing the internet.

Anti-Virus – All capable devices will have anti-virus software. All USB peripherals such as USB drives are to be scanned for viruses before use e.g. when pupils are providing their homework on one.

Safe Use

Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing this E-safety and the staff Code of Practice; pupils upon signing, along with their parents, and returning their acceptance of the Code of Practice. Wireless access should not be granted to persons who have not accepted the Code of Practice, or visitors whose business is not related to school interests.

Email – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Staff may choose to use a personal email address for school communication in agreement with the Head Teacher. Emails of a personal nature are not permitted. Pupils are not permitted to use the school email system, and will not be given their own email address.

Photos and videos – Digital media such as photos and videos are monitored; all parents must sign a Photo Consent form at the time of admission and is reviewed every 3 years. This includes use of photos and videos for use in promotional material, the school website and other school-related media.

Social Networking – there are many social networking services available; Cuddington and Dinton C of E School is fully supportive of social networking as a tool to engage and collaborate with parents and the wider school community. Use of Twitter services are permitted for use within Cuddington and Dinton C of E School and have been appropriately risk assessed. Our feeds are:

•@CDSUpdate – a secure feed for parents to update on school trips, events or news.

•@F4CADS – an open feed to inform parents and the wider community about fundraising events and efforts.

As a broadcast service, these are used as a one-way communication method in order to share school information with the wider school community. No persons will be “followed” or “friended” on these services. Both feeds are used in conjunction with the secure parent Twitter Registration process and the F4CADS Twitter Policy & Agreement.

Governors, Staff and Parents are all aware of how their professional and personal use of social media can reflect on the school and therefore we ask for the utmost vigilance in ensuring it is used:

- Legally
- Securely
- Without undermining the school
- Effectively and
- In a spirit of co-operation and our school values.

Parents of pupils no longer at the school and staff no longer at the school will be deleted from the school Twitter account when they have left.

Mobile Phones - Staff are not permitted to use their mobile phones in school during teaching time when they should be switched off or on silent mode. On some occasions staff may carry phones for safety reasons, for example, when teaching on the field or whilst on a trip. Staff should never take photographs of children on their phone or on a personal device. The school mobile phone should be used for all visits and photographs can be taken on this for school use only.
Visitors will be asked not to use their mobile phones on site whilst children are on site and phones should therefore be turned off or on silent mode.

Incidents - Any E-safety incident is to be brought to the immediate attention of the Head or Designated Safeguarding Lead in their absence.

Training and Curriculum - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, Cuddington and Dinton C of E School will provide opportunities for all stakeholders to trained and updated in developing technologies and e-safety.

E-safety for pupils is embedded into the curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the pupil's learning and posters with reminders will be readily displayed and discussed with children.

E-safety video clips can be found on the school website.