Cavendish Church of England Primary School

E-Safety Policy

This policy should be read in conjunction with Safeguarding Policy, Anti-Bullying Policy, Behaviour Policy and Acceptable Use of WiFi Policy.

Signed: Chair of Governors	
Signed: Headteacher	
Date:	Summer Term 2021
Date to be Reviewed:	Summer Term 2022

Our Vision

In our school our Christian vision shapes all we do.

Challenge, Creativity, Compassion: Create a pure heart in me – Psalm 51:10

Our School Vision Statement reflects this commitment as children and staff are taught to challenge inequality, prejudice, bullying and harm; to respond with compassion and sensitivity to individual need and to respect the rights of all individuals to be safe and nurtured within God's world.

We encourage children to respond creatively to internal and external challenges in life, with compassion for others, including consideration for creation and the planet itself. Thus we show how to live justly and with a pure heart, reflecting the teachings of Jesus and God's love within our school environment.

Introduction and Ethos

At Cavendish CofE Primary School we are committed to promoting the safety and well-being of our school community. We are committed to using new and emerging technologies to drive forward education and are innovative in the use of this technology to help to deliver a creative and educationally stimulating balanced curriculum. We are appreciative of the wealth of information which the use of these technologies can bring to aid teaching and learning. With this in mind, we are knowledgeable about the potential hazards, dilemmas and dangers which our community may face when using new technologies. To be successful we recognise that our ethos needs to be clear and understood by all stakeholders especially students, staff, parents and carers.

Aims and Objectives

To ensure that members of our school community are safe, knowledgeable and responsible users of e-technology.

The specific objectives are as follows:

1. To make staff and students aware of the need for safeguarding themselves when using new and emerging technologies.
2. To help raise parental/carer awareness regarding safe internet use throughout their child's school life.
3. To provide and promote opportunities to raise staff, student and parent/carer awareness of new and emerging technologies.
4. To ensure care when inputting personal information, or when using the internet.
5. To use new and emerging technologies to actively support the curriculum.
6. We are committed to ensuring safeguarding and child protection procedures are followed at all times. This school is mindful of and actively supports the Prevent initiative to guard against radicalisation and extremism.
7. We ensure in our own use that we adhere to GDPR guidelines.

Equal Opportunities

We will ensure that technology, information, advice and guidance is available to, and accessible by, all members of the school community. We are inclusive in our provision of E-Safety and pay special attention to the needs of minority groups, those with protected characteristics or additional needs.

Staff Responsibility and Development

C. Wass	-	Named person for safeguarding (DSL) and safer recruitment, Prevent Duty
A. Lewis	-	Alternative designated named person, Prevent Duty
A. Lewis	-	e-safety
R. Fitzpatrick (Chair of Governors)	-	Safer recruitment
R. Fitzpatrick	-	Safeguarding and Child Protection Governor

Suffolk County Council and ICT Support are available to offer guidance and support on the use of new and emerging technologies and software. A training programme for the use of new resources will be put in place as and when required.

We support staff training opportunities on the use of new and emerging technologies. Any member of staff wishing to apply for training offered by an external provider will need to apply using the established system.

E-mail
E-mail is an essential means of communication throughout the school community. Directed e-mail use can bring significant educational benefits to the learning environment. E-mail should not be considered private and the school reserves the right to monitor e-mail.

- All users are provided with an approved e-mail account within the school environment.
- If an offensive e-mail is received students must immediately inform their teacher; staff must inform the Headteacher.
- Users must not send material or attachments in an e-mail that the receiver may find offensive.
- Students will are advised not to reveal personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission from parents/carers.
- Any staff communication with students and/parents through email must be from the school's approved admin e-mail account.
- Users must not use school email to incite hatred, prejudice or extremism as outlined in the Prevent Duty and DDA.
- Staff may not use private email to send, discuss or communicate school matters.
- Whilst parents may communicate via the website or Google Classroom, school response should be by email (unless marking or feedback related to work content on Google classroom).

School Website
- The contact details on the website include the school address, e-mail and telephone number.
- Any student images will be checked to ensure they have relevant permission for publication.
- Whilst students are required to be at least 13 years old to establish a Facebook account and other social media platforms, we acknowledge that much younger students use this social networking site and have access to others. Therefore we will introduce students to safe use of social media from KS2, including how to guard against extremism.
- The school website has links to school approved learning sites including Google Classroom.

Images
Images of students will not be published on the school website without the permission of the parent/carer. Students will be advised about the reasons for caution in publishing personal information and images in social publishing sites.
- Images that include students will be selected carefully and will not enable individual students to be clearly identified unless written permission has been obtained from parents/carers.
- Students' full names will not be used anywhere on the school's websites or blogs, particularly in association with photographs.
- Parents sign to give permission for use of images in the Pupil Permission Form. This is reviewed annually.

Google Classroom
The school uses an authorised provider for remote learning – Google Classroom. Expectations for children's behaviour and comments are consistent to those taught throughout the school. Children's settings ensure that only class chat is possible and is monitored by the class teacher. The ability for children to talk privately has been disabled. All work set and submitted and any comments go via the Headteacher email for monitoring.

Social Networking and Personal Publishing
Parents/carers and members of the school community need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unchecked content.
- The school reserves the right to block or filter access to social networking sites if the need arises.
- Students and staff will be advised never to give out personal details of any kind which may identify themselves or others and/or their location. Examples would include real name, address, mobile or

landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs.
- Users should be advised to place only appropriate images or footage on any social networking space. They should consider how public the information is and consider using private areas. Advice will be given regarding background detail in a photograph which could identify the student or his/her location (e.g. house number, street name or school).
- Teachers must not run social networking spaces for student use on a personal basis.
- Staff should not add current students to, or become members of, their social networking sites.
- Pornographic sites should not be accessed under any circumstances.
- All users will be advised on security, encouraged to set passwords and not share this information.
- Any personal use of social networking and publishing by staff must not conflict with the ethos of the school or any aspect of the Teaching Standards especially with regards to Part 2.
- The school is aware that bullying can take place through social networking and other online activities. Users will be made aware of methods to deal with cyber-bullying. Parents/carers or the police will be informed, as appropriate, by the Designated Safeguarding Lead.
- Staff have a duty of care to refer any activity which incites prejudice, hatred or intolerance.

Filtering
- The school uses Suffolk County Council's filtering services.
- If students or staff discover unsuitable sites, the web address must be reported to the E-Safety Co-ordinator or Headteacher. All children's laptops are fitted with the 'Dolphin' symbol to report.
- The E-Safety Co-ordinator and Computing Network Manager will monitor the filtering methods.
- Any material that the school believes is illegal must be reported to appropriate agencies.

Mobile Phones (and any other technology)
- Mobile phones should not be used in teaching spaces. Staff are requested to be mindful of others when using phones in the staffroom.
- Staff on visits will be issued with a school mobile phone, when contact with students or parents/carers may be required.
- If contact with students is necessary, staff must use school-owned equipment unless there is an emergency situation in which case the Headteacher should also be informed.
- Any mobiles or mobile devices brought into school by students must be handed into the school office on arrival and collected on their departure from the school. No use of personal technology to be allowed on the school premises by students.
- Any adult wishing to use a personal device on site must sign and agree to the Acceptable Use of Wi-Fi Policy.

Emerging Technologies
Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, wide Internet access and multimedia.
- Emerging technologies will be assessed for educational benefit.
- A data privacy impact assessment will be completed prior to using any data with new technology or IT.
- Any third party provider must be authorised by the Data Protection Officer and meet GDPR criteria including privacy.

Protecting Personal Data
The quantity and variety of data held on students, families and staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused. The Data Protection Act 2018 and GDPR 2018 gives individuals the right to know what information is held about them and it provides a framework to ensure that personal information is handled properly.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 and the school's published Privacy Notice.

Policy Decisions
- The school will maintain a current record of all members of the school community who are granted access to the school's information services and network.

- All staff must read and sign the 'Staff Acceptable Use Policy' and read the e-Safety Policy before using any school Computing resource. These documents will be reviewed annually.
- Students must sign the Acceptable Use Policy, in conjunction with their parent/carer in order to gain access to the Internet facility.
- Staff and contractors with access to school data will sign the Statement of Confidentiality.

Internet Use in the Community
- Any external, authorised access to the school's systems should be within the framework of the Acceptable Use Policy.

Communication to the School Community
- The Headteacher will ensure that an appropriate person attends e-safety training.
- The e-Safety Co-ordinator will introduce the e-Safety Policy and the Acceptable Use Policy to all Year 5 and 6 students, on an annual basis. E-Safety is an integrated component of the computing curriculum and is explicitly revisited each year through safer internet day and is taught as a learning unit in computing in Autumn Term 1 in all classes.
- Staff should understand that the misuse of Information Systems by employees will be treated extremely seriously.
- If a member of staff is concerned about any aspect of their IT use in school, they should discuss this with their line manager to avoid any possible misunderstanding.
- Induction of new staff should include a briefing about the school's e-Safety Policy.
- We acknowledge that e-mail can be an effective method to communicate information related to school matters. In such instances, staff must only send and receive emails from their authorised school email address eg, teacher/LSA to teacher/LSA. However no child's name should be used. Confidential emails to external professionals should be sent via the admin email address which has access to secure portals such as Egress.
- Students are repeatedly made aware of the protocols regarding acceptable email use e.g. language.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- When discussing a pupil's progress with parents, it is preferable to meet face to face or via telephone.

Parent/Carer Involvement
- Parents'/carers' attention will be drawn to the school's e-Safety Policy in the school prospectus and on the school website.
- A partnership approach with parents/carers will be encouraged. This will include an e-safety information leaflet, delivered by the e-Safety Co-ordinator, in conjunction with relevant external agencies, where appropriate.
- By signing the Home-School Agreement, parents and carers give explicit recognition of their duty to promote E-safety and acceptable use at home.
- Parental involvement in Safer Internet Day – activities and information sent home.

This policy will be reviewed on an annual basis by the e-Safety Co-ordinator, the Computing Network Manager and staff Subject Lead for computing.

Behaviour and Cyber-bullying
Cyber-Bullying is defined as the use of Technology (Computing), particularly mobile phones and the internet, with deliberate intent to provoke or cause upset. It can be an extension of face-to-face bullying, with technology providing the bully with another route to harass their target. However, it differs in several significant ways from other kinds of bullying, namely the invasion of home and personal space; the difficulty in controlling electronically circulated messages; the size of the audience; perceived anonymity; and even the profile of the person doing the bullying and their target. Increasingly, exclusion from group chat and social media groups or non-response to communication can be interpretated as a deliberate intent to cause emotional harm and upset.

Cyber Bullying can also affect members of staff and other adults; where staff can be ridiculed, threatened and otherwise abused online by students/parents. The school will take whatever action is necessary to address bullying whether face to face or online. Parents and carers will be informed unless it is felt that

this would put a young person at further risk or if advised not to do so by a partner agency. The school has a statutory duty to report any activity which is illegal or would be covered by the school Safeguarding and Child Protection Policy. The Police will be informed where an offence is thought to have been committed. A list of possible sanctions is available in the school Behaviour Policy.
See Anti-bullying and Safeguarding policy.

Grooming
Grooming refers to actions deliberately undertaken with the aim of befriending and establishing an emotional connection with a child, in order to lower the child's inhibitions in preparation for sexual abuse. We are aware that students may use chat rooms at home and we provide information to inform students about how to protect themselves. Students sometimes speak about the friends which they have made – including 'virtual friends'. Possible warning signs that a student may be being groomed are:

- If their 'friend' is insisting on having their address or phone number.
- If their friend has emailed pictures which made them feel uncomfortable and they would not be able to show to anyone else.
- If the child mentions that they have been asked to email their 'friend' pictures of themselves or use a webcam in a way which makes them feel uncomfortable.
- If their 'friend' has asked them to keep their chats secret.
- If their 'friend' says they will get in trouble for telling an adult what has been going on.
- If their 'friend' wants to meet them and tells them not to let anyone know.

In all these situations an immediate referral should be made to the senior designated professional for Child Protection. Parents will be contacted and Police informed, as necessary.

Peer on Peer Abuse
Peer on Peer Abuse where the protagonist is also a child under the age of 18 is also unacceptable and is covered by legislation outlined in KCSiE (revised annually). Designated Safeguarding Leads must be informed for appropriate referral.

Prevent Duty
As part of the school's proactive stance in fulfilling its Prevent Duty, guidance is given to children about evaluating site content and guarding against hatred, prejudice and extremism of any kind which is contrary to British Laws and Values.

Promotion of E-Safety
As a school, we will use the following strategies:

- Internet Safety Week each February
- Anti-bullying Week each October
- Publication of the e-policy – on the school website
- Publication of e-safety leaflet written and reviewed annually by staff and children
- Annual parental information leaflet on e-safety
- Collective Worship
- Taught curriculum sessions on computing and ICT as appropriate to age group
- Taught curriculum sessions as part of PSHE
- Keeping a log in the safeguarding folder and monitoring incidents of misuse and conduct

Monitoring and Review
This policy is renewed annually as part of the Computing monitoring cycle and safeguarding return.