Fairhaven CEVA Primary School

Internet Acceptable Use Policy

Date Agreed by Governors: 30/01/2020

Date Agreed by staff: 09/01/2020

Date for Review: Autumn Term 2022

31-1-20

Vision Statement

Our Christian school community strives to provide a variety of learning experiences for all our young people. We are here to nurture the gifts God gives us and to celebrate our differences. We encourage our pupils to explore their interests, find their talents, flourish and live life to the full. We want our children to live great lives and ultimately make a difference in the world.

Belief – Friendship – Diversity - Achieve

Statement of Intent

At Fairhaven, we understand that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open up opportunities for pupils and play an important role in their everyday lives.

Whilst the school recognises the importance of promoting the use of computer technology throughout the curriculum, we also understand the need for safe internet access and appropriate use. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff. The school is committed to providing a safe learning and teaching environment for all pupils and staff, and has implemented important controls to prevent any harmful risks.

Legal Framework

This policy has due regard to the following legislation, including, but not limited to:

- The General Data Protection Regulation
- Human Rights Act 1998
- Data Protection Act 1998
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Safeguarding Vulnerable Groups Act 2006
- Education and Inspections Act 2006
- Computer Misuse Act 1990, amended by the Police and Justice Act 2006
- Communications Act 2003
- Protection of Children Act 1978
- Protection from Harassment Act 1997

This policy also has regard to the following statutory guidance:

- DfE (2018) 'Keeping children safe in education'

This policy will be used in conjunction with the following school policies and procedures:

- E-security Policy
- Digital Safeguarding Policy
- Cyber Bullying Policy
- Social Media Policy
- Allegations of Abuse Against Staff Policy
- Acceptable Use Agreement

Use of the Internet

The purpose of Internet use in school is to promote pupil achievement, to support the professional work of staff and to enhance the school's management, information and business administration systems. Benefits of using the Internet in education include:

- Access to world-wide educational resources
- Access to subscription based educational websites
- Educational and cultural exchanges between pupils world-wide
- Access to experts in many fields for pupils and staff
- Staff professional development through access to national developments, educational materials and good curriculum practice
- Communication with support services, professional associations and colleagues
- Exchange of curriculum and administration data with the LEA and DfES.

The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using ICT across computer networks including the internet. Consequently, in delivering the curriculum teachers need to plan to integrate the use of communication and collaborative technology such as web-based resources and e-mail to enrich and extend learning activities. Effective Internet use is an essential life-skill for all pupils to master.

When accessing the internet, individuals are especially vulnerable to a number of risks which maybe physically and emotionally harmful, including:

- Access to illegal, harmful or inappropriate images
- Cyber bullying
- Access to, or loss of, personal information
- Access to unsuitable online videos or games
- Loss of personal images
- Inappropriate communication with others
- Illegal downloading of files
- Exposure to explicit or harmful content, e.g. involving radicalisation
- Plagiarism and copyright infringement

- Sharing the personal information of others without the individual's consent or knowledge

Roles and responsibilities

It is the responsibility of all staff to be alert to possible harm to pupils or staff due to inappropriate internet access or use, both inside and outside of the school, and to deal with incidents of such as a priority. The governing body is responsible for ensuring that there are appropriate filtering and monitoring systems in place to safeguard pupils.

The e-safety officer is responsible for:

- ensuring the day-to-day e-safety in the school, and managing any issues that may arise.
- the provision of all relevant training and advice for members of staff as part of the requirement for staff to undergo regularly updated safeguarding training and be able to teach pupils about online safety.
- regular monitoring the provision of e-safety in the school and will provide feedback to the Head Teacher.
- maintaining a log of submitted e-safety reports and incidents.
- ensuring that all members of staff are aware of the procedure when reporting e-safety incidents, and will keep a log of all incidents recorded. Cyber bullying incidents will be reported in accordance with the school's Anti-Bullying and Harassment Policy.

The Head Teacher is responsible for:

- ensuring that the e-safety officer and any other relevant staff receive CPD to allow them to fulfil their role and train other members of staff.
- (along with the data protection officer (DPO)) ensuring there is a system in place which monitors and supports the e-safety officer, whose role is to carry out the monitoring of e-safety in the school, keeping in mind data protection requirements.
- establishing a procedure for reporting incidents and inappropriate internet use, either by pupils or staff.
- reviewing and amending this policy with the e-safety officer and DPO, taking into account new legislation, government guidance and previously reported incidents, to improve procedures.
- communicating with parents regularly and updating them on current e-safety issues and control measures.

The governing body will:

- meet with the e-safety officer to discuss the effectiveness of the e-safety provision, current issues, and to review incident logs, as part of the school's duty of care.
- evaluate and review this E-Safety Policy, taking into account the latest developments in ICT and the feedback from staff/pupils.

Teachers are responsible for:

- ensuring that e-safety issues are embedded in the curriculum and safe internet access is promoted at all times.

All staff are responsible for:

- ensuring they are up-to-date with current e-safety issues, and this E-Safety Policy.
- ensuring they understand and adhere to our Acceptable Use Agreement, which they must sign and return to the Head Teacher.

Parents are responsible for:

- ensuring their child understands how to use computer technology and other digital devices appropriately.

All pupils are aware of their responsibilities regarding the use of school-based ICT systems and equipment, including their expected behaviour.

E-Safety Education

Pupils

An e-safety programme is taught across the curriculum on a regular basis, ensuring that pupils are aware of the safe use of new technology both inside and outside of the school. They will be taught about the importance of e-safety and are encouraged to be critically aware of the content they access online, including extremist material and the validity of website content. They will also be taught to acknowledge information they access online, in order to avoid copyright infringement and/or plagiarism. Clear guidance of internet use will be presented around school.

Pupils are instructed to report any suspicious use of the internet and digital devices to class teachers and PSHE lessons will be used to educate pupils about cyber bullying, including how to report cyber bullying, the social effects of spending too much time online and where to access help. The school will promote e-safety through. Child Exploitation and On line Protection (CEOPs) training and PSHE lessons.

Staff

All staff will undergo e-safety training to ensure they are aware of current e-safety issues and any changes to the provision of e-safety, as well as current developments in social media and the internet as a whole. They will undertake audits in order to identify areas of training need and employ methods of good practice and act as role models for pupils when using the internet and other digital devices.

All staff are reminded of the importance of acknowledging information they access online, in order to avoid copyright infringement and/or plagiarism. Any new staff are required to undergo e-safety training as part of their induction programme, ensuring they fully understand this E-Safety Policy.

Parents

E-safety information will be directly delivered to parents through a variety of formats, including newsletters, the school website and social media. Parents' evenings, meetings and other similar occasions will be utilised to inform parents of any e-safety related concerns.

Internet Access

Parents will be informed that pupils will be provided with supervised internet access and will be required to sign and return a form **acknowledging their understanding of the school's policy on Internet use**. The school will keep a record of all staff and pupils who are granted Internet access. The record will be monitored by the head/co-ordinator.

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school, with the support and guidance of the LA, will take all precautions to ensure that users only access appropriate material. However, due to the international and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never occur on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.

Internet access can be further controlled whilst using LearnPad tablets which allow staff to create direct links to specific websites that prevent the user from accessing any other parts of the Internet.

If staff or pupils discover unsuitable sites, the URL (address) and content must be reported immediately to the ICT Co-ordinator or Head Teacher. Staff and pupils will be made aware that the use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Staff Access

Staff will be encouraged to use this resource to support and enrich their own teaching and professional development. Staff will observe all restrictions and policies with regards to appropriate use of the internet. Staff
will follow the Guidance for Employees on Internet and E-Mail Use in Schools Section 11 of the Personnel Handbook (amendment MI sheet 100/06). Any complaint about staff misuse must be referred to the Head Teacher.

E-mail

Each member of staff has their own e-mail address on the school's networked system. Only these approved e-mail accounts may be used on the school system.

Social Networking

Use of social media on behalf of the school will be conducted following the processes outlined in our Social Media Policy.

- Access to social networking sites will be filtered as appropriate.

- Should access be needed to social networking sites for any reason, this will be monitored and controlled by staff at all times and must be first authorised by the Head teacher.
- Pupils are regularly educated on the implications of posting personal data online outside of the school.
- Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and the school as a whole.
- Staff are not permitted to communicate with pupils over social networking sites and are reminded to alter their privacy settings.
- Staff are not permitted to publish comments about the school which may affect its reputability.
- Staff are not permitted to access social media sites during teaching hours unless it is justified to be beneficial to the material being taught. This will be discussed with the Head Teacher prior to accessing the social media site.

School Websites

The school website has been created to celebrate children's work, promote the school, publish resources and provide public information for parents and others to directly access e.g. letters and policies etc. Staff and pupil's home/personal information will not be published.

It has been agreed by the governors that photographs of the school and the children can be published with parental consent and careful selection based upon children being reasonably unidentifiable i.e. using profile or distant images together with using a reduced standard of photo quality in order that quality images cannot be reproduced. Names of children will never be linked directly with images.

It has been agreed by the governors that with parental permission children's first names (and the first letter of their second name if there are multiples of children with the same name) can be published on the school website when linked to work, news or their web page etc.

Parental consent for the use of the first names, work and selected photographs of pupils to be used on the school website in accordance with this policy, will be sought for each pupil on their admission to the school.

Children will be made aware of their responsibility by staff, not to name themselves or others on the website or attempt to publish any personal information or make any personal comments about themselves or others. Class teachers will hold the publishing rights to all information submitted by pupils to the website.

The Head Teacher, co-ordinator and bursar will monitor all contributions to the website.

Network Security

Network profiles for each pupil and staff member are created in which the individual must enter a username and personal password when accessing the ICT systems within the school. The e-safety officer and ICT technicians (NetCentral) will ensure all school-owned laptops and computers have their encryption settings turned on or, if there is no built-in encryption option, encryption software is installed. Important folders, e.g. those including pupils' medical records, will be password protected to ensure their security – the e-safety officer and other designated individual(s) will be the only people who have access to this password.

Virus Management

Technical security features, such as virus software, are kept up-to-date and managed by ICT technicians (NetCentral). The ICT technicians (NetCentral) in conjunction with the e-safety officer will ensure that the filtering of websites and downloads is up-to-date and monitored. Firewalls will be switched on at all times – ICT technicians will review these on a weekly basis to ensure they are running correctly and to carry out any required updates. Firewalls and other virus management systems, e.g. anti-virus software, will be maintained in accordance with the school's Data Security Breach Prevention and Management Plan. Staff members will report all malware and virus attacks to the e-safety officer, ICT technicians (NetCentral) and DPO immediately.

School Rules

The school has developed a set of guidelines for Internet use by pupils. These rules will be made available to pupils and kept under constant review. All members of staff are responsible for explaining the rules and their implications. All members of staff need to be aware of possible misuses and their responsibilities towards pupils.

The following rules apply to all pupils:

- I will ask permission before entering any web site, unless my teacher has already approved that site.
- I will only use my own login and password, which I will keep secret.
- I will not look at or delete other people's files.
- I will not bring CDs or portable storage devices into school without permission.
- I will only e-mail people I know, or my teacher has approved.
- The messages I send will be polite and sensible.
- When sending an e-mail, I will not give my home address or phone number, or arrange to meet someone.
- I will ask for permission before opening an e-mail or an e-mail attachment sent by someone I do not know.
- I will not use Internet chat.
- If I see anything I am unhappy with, or I receive messages I do not like, I will tell a teacher immediately.
- I will not enter personal information about myself, others or make any personal comment about others and I will only use first names when necessary and with a teacher's permission.

- I know that the school may check my computer files and may monitor the Internet sites I visit.
- I understand that if I deliberately break these rules, I could be stopped from using the Internet or computers.

Sanctions

1. Violations of the above rules will result in a temporary or permanent ban on Internet use.
2. Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour.
3. When applicable, police or local authorities may have to be involved.

Appendix 1

Dear Parents/Carers

Pupil Use of the Internet at School

As part of the National Curriculum pupils will be provided with supervised access to the Internet. We believe that use of the World Wide Web and e-mail is worthwhile and is an essential skill for children as they grow up in the modern world. They will be able to obtain a rich variety of resources from around the globe to enhance their studies as they research information from museums, libraries, educational organisations and a range of other suitable web sites. They will also learn to exchange e-mails with pupils in partner schools. The pupils will also have the opportunity to contribute to their own page on the school website and therefore be able to contribute directly to the World Wide Web.

Although there have been concerns about pupils having access to undesirable materials, we constantly review the risks in school and actively undertake all possible precautions to reduce identified risks. Our access to the Internet comes through Exa Education and our content is filtered by SurfProtect which is monitored by Netcentral, our IT support company.

Children will be introduced to a set of rules and taught how to use the Internet responsibly by using the safe environment of the Intranet. When they are given access to the Internet they will be supervised and directed towards specific curriculum activities and suitable web sites. However, the school cannot be held responsible for the nature or content of materials accessed through the Internet. The school will not be liable for any damages arising from your child's use of the Internet facilities.

I enclose a copy of the school's Internet Acceptable Use Policy and rules for using the Internet. Children and their parents/guardians need to read the policy and rules and agree to them by signing and returning the pupil, parent/guardian and school website agreement forms before access to the Internet will be granted to the pupil.

Should you wish to discuss any aspect of our use of the Internet please telephone me to arrange an appointment.

Yours sincerely

Mrs S. Lake
HEAD TEACHER

Appendix 2

Pupil's Acceptance of the School's Internet Acceptable Use Policy

Please complete and return this form to your child's class teacher.

Pupil's agreement:

I have read and understood the school rules for Responsible Internet Use. I will use the computer system and Internet in a responsible way and obey these rules at all times. I understand that if I break these rules then I may not be allowed to use the Internet.

Pupil's signature _____ Date ___/___/___

Parent's/Carer's agreement:

I have read and understood the school rules for responsible Internet use and give permission for my son/daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I understand that the school is not liable for any damages arising from the use of Internet facilities.

Parent's/Carer's signature _____ Date ___/___/___

Name of Pupil _____

Class _____