Cherrywood Community Primary School

E-Safety Policy

INTRODUCTION

This policy sets out the ways in which the school will:

- educate all members of the school community on their rights and responsibilities with the use of technology;
- build both an infrastructure and culture of e-Safety;
- work to empower the school community to use the Internet as an essential tool for life-long learning.

The E-Safety Policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers and visitors) who have access to and are users of school ICT systems. The policy highlights the need to educate pupils about the benefits and risks of using technology and provide safeguards and awareness for users to enable them to control their online experience.

AIMS

The aims of the school are to help every pupil and adult to:

- Feel safe and confident when using new technologies.
- Know who to speak to when they feel unsafe.
- Know how to report any abusive behaviour.
- Know how to use the internet correctly, without misuse.
- Stay in control and keep personal information private.
- How to take the necessary measures to block and delete accounts, messages and people.

ROLES AND RESPONSIBILITIES

Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. The Property Asset Management Committee (PAM) will receive regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken the role of E-Safety Governor with responsibilities for the following: -

- Meetings with the E-Safety Co-ordinator.
- Monitoring of E-Safety incident logs / filtering / change control logs.
- Reporting relevant information to the PAM.

Headteacher and Senior Leadership Team

The Headteacher has overall responsibility for E-Safety, although day to day management affairs have been delegated to the E-Safety Co-ordinator.

The Headteacher and Senior Leadership Team are responsible for ensuring that all staff and the E-Safety Co-ordinator receive correct and suitable Continuing Professional Development (CPD).

The Headteacher and Senior Leadership Team will ensure that there is a system in place to monitor the usage of internet and other technologies and that the person who carries out the internal E-Safety monitoring receives support and is also monitored. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

The Headteacher and Senior Leadership Team will ensure that they receive regular updates and reports from the E-Safety Co-ordinator.

The Headteacher and Senior Leadership Team are to ensure they know the correct procedures that need to be followed when a serious allegation has been made by a child or one that is in regards to a member of a staff.

E-Safety Co-ordinator

The E-Safety Co-ordinator will take day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school E-Safety policies / documents.

The E-Safety Co-ordinator will ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place and will provide training and advice for all staff.

The E-Safety Co-ordinator will liaise with the Local Authority and with ICT technical staff.

The E-Safety Co-ordinator will receive reports of E-Safety incidents and create a log of incidents to inform future e-safety developments.

The E-Safety Co-ordinator will report regularly with Governors to discuss current issues, review incident logs and filtering / change control logs and reports regularly to Senior Leadership Team.

Technical Staff

The school uses Hampshire County Council's ICT services and therefore is required to comply with their email, internet and intranet policies. The HCC filtering facility software is used in order to avoid access to inappropriate sites or material. The school will work in partnership with Hampshire County Council to ensure systems to protect pupils are reviewed and improved.

Harrop will provide technical support for computer equipment that was supplied by them. The services provided by Harrap include: source and supply new hardware, provide

weekly on-site support, install and upgrade software, troubleshoot technical problems, maintain the network, offer technical advice over the telephone and provide advice on strategic management of resources.

The school will comply with their “Policy on Staff Acceptable Use of ICT” and any relevant Local Authority E-Safety Policies / guidance.

Teaching and Support Staff

E-safety will be a focus in all areas of the curriculum and staff will reinforce E-Safety messages in the use of ICT across the curriculum. Teaching and Support Staff are responsible for-

- Stay up to date with current E-Safety matters, policies and practices.
- Read, understand, sign and comply with the “Policy on Staff Acceptable Use of ICT”.
- Report any misuse or problems to the E-Safety Co-ordinator/ Headteacher for further investigation.
- Digital communications with pupils (email, Learning Platform) are strictly professional and only carried out using school systems.
- Pupils are made aware and follow the E-Safety and Acceptable Use policies.
- E-Safety issues relating to the use of mobile phones, cameras and hand held devices are properly monitored in accordance with the school’s policies.

In lessons where internet use is pre-planned, it is best practice that pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches. Where pupils are allowed to freely search the internet (e.g. using search engines) staff should be vigilant in monitoring the content of the websites the pupils visit.

Designated Safeguarding Leaders

The Designated Safeguarding Leaders needs to ensure that school staff are fully trained in E-Safety issues and are aware that serious child protection issues could occur due to: -

- Cyber- bullying.
- Sharing of personal data.
- Inappropriate online conduct with adults/ strangers.
- Potential or actual incidents of grooming.

Pupils/ Students

Pupils and students are responsible for-

- Knowing and acting accordingly to the school’s E-Safety and Acceptable Use Policies.
- Knowing the importance of reporting abuse, misuse or access to inappropriate materials and know how to report them.
- Knowing the policy on mobile phones, digital cameras and other hand held devices and to realise these can be used for cyber-bullying.
- Understanding that the E-Safety policy also covers their actions out of school, if related to their membership of the school.

Parents/ Carers

Parents and carers have the responsibility to ensure that their children use the internet and mobile phones correctly and do not misuse these technologies. Full copies of the E-Safety and Acceptable Use policies are available from the school office and posted on the school's website. Parents/Carers must be aware of these policies and agree to their content by signing the school's Permission Forms.

EDUCATION

Pupils

The Internet is an essential element for education, business and social interaction.
Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils and, as such, the school has a duty to provide pupils with quality Internet access as part of their learning experience in the following ways:-

- The school Internet access will be designed expressly for pupil use including appropriate content filtering.
- Pupils will be given clear objectives for Internet use and taught what use is acceptable and what is not.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- As part of the new ICT curriculum, all year groups will be shown how to focus on the different elements of staying safe on line.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- When children are directed to websites as part of home learning they will have been checked for appropriateness by the teacher setting the learning
- Pupils will be shown how to publish and present information appropriately to a wider audience.

Through ICT, the school will ensure that the needs of all are met, taking account of gender, ethnicity, culture, religion, language, age, ability, disability and social circumstances. It is important that in this school we meet the diverse needs of pupils to ensure inclusion for all and that all pupils are prepared for full participation in a multi-ethnic society.

Parents / Carers

Parents and carers will be informed about the ways the internet and technology is used in school. They have a critical role to play in supporting their children with managing e-Safety risks at home, reinforcing key messages about e-Safety and regulating their home experiences. The school supports parents and carers to do this by:

- Providing clear ICT acceptable use guidance and asking parents / carers to sign the school's Permission Forms.
- Raising awareness through activities planned by pupils;
- Inviting parents to attend activities such as e-Safety and ICT events.

TRAINING OF STAFF AND GOVERNORS

There is a planned programme of e-Safety training for all staff and governors in order to ensure they understand their responsibilities, as outlined in the E-Safety and Acceptable Use policies. This includes:

- An annual audit of the e-Safety training needs for all staff will be carried out.
- All new staff will receive e-Safety training as part of their induction programme.
- The e-Safety Co-ordinator will receive regular updates, through attendance at external training events and by reviewing guidance documents released from Hampshire County Council and other relevant organisations.
- This e-Safety Policy and its updates will be shared and discussed at staff meetings.
- The e-Safety Co-ordinator will provide advice/guidance/training to individuals as required.

Governors will take part in e-safety training / awareness sessions, in the following ways:

- Attendance at training provided by the Local Authority / National Governors Association or other relevant organisation.
- Participation in school training / information sessions for staff or parents, including attendance at assemblies / lessons.

TECHNICAL INFRASTRUCTURE

When working with the technical support provider, the school will ensure that the following guidelines are adhered to: -

- The School ICT systems are managed in ways that ensure that the school meets e-Safety technical requirements
- There are regular reviews and audits of the safety and security of school ICT systems.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and work stations from accidental or malicious attempts which might threaten the security of the school systems and data.
- The school will ensure that regular reviews are made to ensure that the filtering methods are appropriate, effective and reasonable.

The “Policy on Staff Acceptable Use of ICT” provides clear explanations on technical and security aspects, including Access (Section 3), Unacceptable use (Section 8) Personal and private use (Section 9) Security and confidentiality (Section 10) and Monitoring (Section 11). The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that the Acceptable Use and E-Safety policies are implemented. It will also ensure that the relevant staff will be effective in carrying out their e-safety responsibilities.

DATA PROTECTION

The Data Protection Policy sets out how the school deals with personal information correctly and securely in accordance with the Data Protection Act 1998 and other related legislation. In relation to E-Security, the school will adhere to the following: -

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices.

- Ensure that users are properly “logged-off” at the end of any session in which they are accessing personal data.
- Store or transfer confidential data using encryption and secure password protected devices.
- Make sure data is deleted from the device once it has been transferred or its use is complete.

USE OF DIGITAL AND VIDEO IMAGES

Photographs and videos taken within school are used to support learning experiences across the curriculum, to share learning with parents and carers on our school’s website and to provide information about the school on the website. The school will:

- When using digital images, instruct staff to educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images including on social networking sites.
- Allow staff to take images to support educational aims, but make sure that images or videos that include pupils will be selected carefully and will not provide material that could be reused.
- Make sure that pupils’ full names will not be used anywhere on the school website, particularly in association with photographs.
- Written permission from parents or carers will be obtained via the Parents and Permission Form before images or videos of pupils are electronically published.
- Keep the written consent where pupils’ images are used for publicity purposes, until the image is no longer in use.
- Staff will not keep images of children on personal devices e.g. memory sticks, or use them for any use other than in school.

ZAPPAR

Zappar produces bite-sized entertainment experiences using image recognition technology to provide a platform for products – in other words 3D augmented reality. Scannable zapcodes are used to show digital content.

User Generated Content may contain or depict personal details e.g. audio, photos or videos featuring pupils. Cherrywood will be responsible for and be selective about what personal details are put into User Generated Content. Personal information, such as telephone numbers, physical addresses, full name or any other information of a sensitive nature, will not be submitted to any publicly available area of the ZAPPAR Services.

COMMUNICATION

A wide range of rapidly developing communications technologies has the potential to enhance learning. The “Policy on Staff Acceptable Use of ICT” provides clear guidance on the acceptable use of these technologies, including e-mails, mobile phones, school telephones, internet and social networking. The Acceptable Use Policy also provides information to staff on ways to protect themselves from inappropriate use of ICT resources and equipment. The school will be responsible for ensuring that the Acceptable Use and E-Safety policies are effectively implemented.

ASSESSMENT OF RISK

Methods to identify, assess and minimise risks will be reviewed regularly. As technology advances the school will examine and adjust the e-Safety Policy. Part of this consideration will include a risk assessment:

- looking at the educational benefit of the technology; and
- considering whether the technology has access to inappropriate material.

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the global and connected nature of internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor Hampshire County Council can accept liability for the material accessed, or any consequences resulting from internet use.

All users need to be reminded that the use of computer systems, without permission or for inappropriate purposes, could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to Police.

REPORTING AND RESPONSE TO INCIDENTS

The school will respond to illegal and inappropriate incidents as follows: -

- Incidents of internet misuse by pupils and staff will be referred to the headteacher.
- All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyber bullying, illegal content etc).
- Pupils and parents will be informed of the consequences for pupil misuse of the Internet (refer to Acceptable Use Policy).
- The e-Safety Co-ordinator will record all reported incidents and actions taken in the School e-Safety incident log and in any other relevant areas e.g. Bullying or Child Protection log.
- The designated Child Protection Coordinator will be informed of any e-Safety incidents involving child protection concerns, which will then be escalated in accordance with school's Child Protection Policy.
- The school will inform parents and carers of any incidents or concerns in accordance with school procedures.
- If investigations are needed, the school will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern that illegal activity has taken place (or the school is unsure how to proceed with any incidents of concern), then the school will contact the Hampshire County Council Children Services Team for support.

The police will be informed where users visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- child sexual abuse images;
- promotion or conduct of illegal acts, under the child protection, obscenity, computer misuse and fraud legislation;
- adult material that potentially breaches the Obscene Publications Act in the UK;
- criminally racist material.

COMMUNICATION OF POLICY

Pupils

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that Internet use will be monitored.

Staff

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Parents

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school prospectus and on the school Web site.

SANCTIONS AND DISCIPLINARY PROCEEDINGS

Sanctions and disciplinary procedures will be taken where users visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- pornography, adult or mature content;
- promotion of any kind of discrimination, racial or religious hatred;
- personal gambling or betting;
- personal use of auction sites;
- any site engaging in or encouraging illegal activity;
- threatening behaviour, including promotion of physical violence or mental harm;
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute;
- use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Hampshire County Council and the school;
- uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions;
- revealing or publicising confidential or proprietary information (e.g. financial or personal information, databases, computer or network access codes and passwords);
- creating or propagating computer viruses or other harmful files;

OTHER SCHOOL POLICIES

This policy should be read in conjunction with other school policies, including the Staff Acceptable Use of ICT, Child Protection, Anti Bullying, PHSE, Confidentiality, Whistle Blowing, Equality and Data Protection policies.

This policy was adopted on : 11th April 2016

Next review date : April 2018, thereafter every two years

Signed by :
Betty Read (on behalf of the Governing Body)