ESafety Policy 2021-2022

Review date: Sept 2022

Policy Statement

At Cam Woodfield Junior School, 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 an annual basis or in response to an e-safety incident, whichever is sooner.

The primary purpose of this policy is twofold:

- To ensure the requirement to entrust the whole school community with the ability to stay safe and risk free.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce the potential of harm to the pupil or liability to the school.

Upon review all members of staff will sign as read and understood both the e-safety policy and the Staff Acceptable Use Policy. A copy of the Pupils' E-Safety agreement will be sent home with pupils at the beginning of each school year with a permission slip. Upon return of the signed permission slip and acceptance of the terms and conditions, pupils will be permitted access to school technology including the Internet.

Introduction

Information Technology (IT) in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Schools need to build in the use of these technologies in order to enable our young people with the skills to access life-long learning and employment.

At Cam Woodfield Junior School, we understand the responsibility to educate our pupils on e-Safety issues: teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, whilst in and beyond the classroom. Using the National Curriculum and the KCSIE 2021 documentation, the school has devised a programme of study for the children to follow as they progress through the school.

Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of:

- Fixed Internet (LAN and WiFi).
- Mobile Internet
- Technologies provided by the School (such as PCs, laptops, tablets and interactive whiteboards/TVs)

Policy Governance (Roles & Responsibilities)

As e-Safety is an important aspect of strategic leadership within the school, the Head and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The Computing lead, alongside the teaching staff, are to ensure the safety of pupils online is monitored and any issues arising will be to notify the Head immediately.

Teaching staff and Governors are updated by the Head /Computing lead and all Governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the School's Acceptable Use Agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: KCSIE documentation, child protection, health and safety, home-school agreements, and behaviour/pupil discipline (including the anti-bullying) policy**.**

Why is Internet use important?

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- The school has a duty to provide students with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How does the Internet benefit education?

- Access to world-wide educational resources including museums and art galleries.
- Cultural, vocational, social and leisure use in libraries, clubs and at home.
- Access to experts in many fields for pupils and staff.
- Professional development for staff through access to national developments, educational materials and effective curriculum practice.
- Collaboration with support services, professional associations and colleagues.
- Improved access to technical support including remote management of networks and automatic system updates.
- Access to learning wherever and whenever convenient.

How can the Internet enhance learning?

- The School Internet access is designed for pupil use and includes filtering appropriate to the age of pupils.
- Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and ability.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluated.
- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to the Site Manager and Computing lead.
- Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.

- Pupils should be taught to be aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of on-line materials is a part of every subject.

How will ICT system security be maintained?

- The security of the school ICT systems will be reviewed regularly.
- Virus and ransomware protection will be installed and updated regularly.
- Personal data sent over the Internet will be encrypted or otherwise secured.
- Use of portable media will be reviewed. Portable media may not be used without specific permission and a virus check.
- Files held on the school's network will be regularly checked.
- The dedicated IT technician will review system capacity regularly.

How will e-mail be managed?

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone .
- Whole-class or group e-mail addresses can be created for pupils use when learning about emails and will need to be setup by the Site Manager.
- Access in school to external personal e-mail accounts may be blocked.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- Reference to e-mail usage for staff can be found in the Communications Policy.

** For children, emailing will be taught through the safe environment of e-Schools VLE**

How will published content be managed?

- The contact details on the website should be the school address, e-mail and telephone number.
- Staff or pupils personal information will not be published.
- Email addresses should be published carefully, to avoid spam harvesting.
- The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

Can pupil's images or work be published?

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified unless written permission has been given to the school.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Pupils learning outcomes may be shared online and celebrated on year group blogs.

How will social networking and personal publishing be managed?

- Pupils are advised never to give out personal details of any kind, which may identify them or their location. Examples would include real name, address, contact phone numbers, school, e-mail address, names of friends, specific interests and clubs etc.
- Pupils will be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g. House number, street name, school, shopping centre.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.
- Pupils should be advised not to publish specific and detailed private thoughts.
- We are aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.
- The school's PSHE scheme of work and Computing curriculum has been extended to incorporate the education of children on the Internet and its safe use.

How will filtering be managed?

- We will work in partnership with parents, the LEA, DfE and our ICT support provider, to ensure systems to protect pupils are reviewed and improved
- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to the Headteacher and Computing lead. Children will be educated as to the correct and safe procedure to do this
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable
- Any material that the school believes is illegal must be referred to the Internet Service Provider.
- Filtering strategies will be selected by the school, in discussion with the filtering provider where appropriate.

How can emerging technologies be managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is permitted.
- Staff will be issued with a school phone where contact with pupils is required.

How should personal data be protected?

The Data Protection legislation requires that data is**:**

- Processed fairly and lawfully
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Held no longer than is necessary
- Processed in line with individual's rights
- Kept secure

- Transferred only to other countries with suitable security measures

How will Internet access be authorised?

- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- Our pupils' access to the Internet will be by adult demonstration with opportunities for the children to work directly on the Internet individually or with a partner. This will always be directly supervised by a teacher or adult.
- Parents will be informed that pupils will be provided with supervised Internet access.
- Parents will be asked to sign and return a consent form.
- Pupils will not be issued individual e-mail accounts, but will be authorised to use a group/class email address under supervision.

How will risks be assessed?

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The Headteacher will ensure that the E-Safety Policy is implemented and compliance with the policy is monitored.

How will e-safety complaints be handled?

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- Discussions will be held with the Police liaison officer to establish procedures for handling potentially illegal issues.
- The Safer Internet police agency will be informed of any potentially unsafe practice.
- CEOPs referral may be made if there is a possibility of exploitation e.g. grooming.

Sanctions within the school discipline policy include:

- interview / counselling by teacher / Headteacher
- informing parents or carers;
- the police may be informed
- removal of Internet or computer access for a period of time

How will the policy be introduced to pupils?

- Rules for safe Internet access will be posted in areas of the school with access to the internet. These rules will be carefully written and illustrated to ensure all children understand their message. Children from the School Council will be involved to ensure these rules are approved by children, for children.
- Pupils will be informed that Internet use will be monitored.
- E-safety will be embedded into the curriculum, raising the awareness and importance of safe and responsible internet use. Instruction in responsible and safe use should precede Internet access. When this policy is released to pupils, staff, parents, the internet will be out of bounds until consent has been received.
- A year group module of the GSP's 'Digital Futures' will be used to teach pupils the importance of wellbeing and self-image when using online material.

How will the policy be discussed with staff?

- All staff must accept the terms of the 'Acceptable Use Policy' statement before using any Internet resource in school.
- All staff will be given the School E-Safety Policy and its importance explained to them. The whole staff will also be involved in the confirmation of the final draft of this policy before release to parents and children.
- Staff will be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- The monitoring of Internet use is a sensitive matter. Members of staff that operate monitoring procedures should be supervised by senior management.
- Staff development in safe and acceptable use of the Internet and on the school E-Safety Policy will be provided as required.

How will parents' support be enlisted?

- Parents' attention will be drawn to the School E-Safety Policy in initial letters and newsletters and from then onwards, the school website.
- The use of School Ping and social media platforms will be used to communicate and identify current online risks.
- Internet issues will be handled sensitively to inform parents without alarm.
- A partnership approach with parents will be encouraged. This includes parent Internet safety information evenings which would include demonstrations, practical activities and suggestions for safe home Internet use.