E-Safety Policy

Autumn 2019 Review Autumn 2020

OUR FEDERATION VISION

Together we will flourish and thrive,

building on our Christian and local community,

for the good of all.

Those who trust in the Lord will find new strength. They will soar high on wings like eagles. Isaiah 40v.31

Our Federation Values are reflected within this policy as it is through our values of *love* and *respect* for ourselves and for others, that no child or adult should use the internet or associated mobile technologies to hurt anyone.

The Kite Primary Federation

E-Safety Policy

Please note: in this policy 'school' refers to any school within the Kite Primary Federation

Introduction

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all are staff are bound. Through this E–Safety Policy, staff will ensure they meet their statutory obligations to ensure that children and young people are safe and protected from harm, both within and outside of the schools. This policy also forms part of our protection from legal challenge, relating to the use of digital technologies.

Scope

This policy applies to all members of our school communities (including staff, pupils, students, volunteers, parents, carers, visitors, and governors) who have access to and are users of the ICT systems, both in and out of the schools.

Rationale

E-safety is about the safety issues associated with information systems and electronic communications as a whole. This encompasses not only the internet but all wireless electronic communications including mobile phones, games consoles, cameras and webcams. It also needs to take into account the increasing mobility of access to digital technology through the range of mobile devices.
It is really important to remember that the issue at hand is not the technology but the behaviour around how we use it; the use of new technologies in education brings more benefits than risks.
Issues relating to e-safety need to be seen as part of the Safeguarding children agenda, not purely ICT. It is the responsibility of all, to understand the risks, acceptable use, as well as how to respond to incidents involving e-Safety, both in and out of the school environment.

Policy development

The E-Safety policy relates to other policies including those for ICT, Anti-bullying and Safeguarding children.

- Our policy has been written with full consultation from staff in school, parents/carers, governors and young people.
- It has been agreed by senior managers and approved by governors
- The policy and its implementation will be reviewed annually
- It is available to read or download on our school website or as a hard copy from the school office

Roles and responsibilities
The schools have an E-Safety coordinator. Our coordinator is: Charlotte Rigby and works closely with the Designated Safeguarding Lead or deputies for safeguarding, (Kathryn King, Sally Beaman and Jane Dorans) and the Data Protection Officer to ensure issues do not arise such as:

- Sharing of data
- Access to inappropriate materials
- Inappropriate on-line contact with adults/ strangers
- Cyber- bullying
- Potential or actual incidents of grooming

Teaching and Learning
Why internet and digital communications are important

- The purpose of any technology in our schools is to raise educational standards, to promote achievement, to support the professional work of staff and to enhance the school's management functions.
- The schools have a duty to provide students with quality internet access as part of their learning experience.
- Internet use is part of the statutory curriculum and a necessary tool for staff.
- Pupils will be educated in the safe, effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- They will be encouraged to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be shown how to publish and present information appropriately to a wider audience.
- They will be taught what internet use is acceptable and what is not and be given clear objectives for use. These are also important transferable skills for their life out of school, including using mobile phones and other mobile devices.
- They will be taught how to report unpleasant internet content including Cyberbullying or unwanted contact. This will include using the CEOP icon or the Hector Protector function.
- Issues such as Cyberbullying and e-safety will be built into the curriculum to encourage self –efficacy and resilience. Some children who have had problems or with additional needs may need additional support.

Managing Internet Access
Information security system

- The school ICT system security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies may be discussed with the Local Authority

E-mail

- Pupils and staff may only use approved e-mail accounts on the school system
- Pupils must immediately tell a member of staff if they receive offensive e-mail.
- Staff to pupil e-mail communication must only take place via a school e-mail address or from within a learning platform and will be monitored
- All incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school will consider how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

Published content and the Kite Primary Federation website

- The contact details on the Federation's website should be the school addresses. No staff or pupil's personal details will be published
- The head teacher has overall editorial responsibility to ensure that content is accurate and appropriate.

Publishing pupils' images and work

- Photographs that include children will be selected carefully and will not enable individuals to be clearly identified. Group photographs will be used if possible rather than full-face photos of individual children.
- Pupil's full names will not be used on the Federation website and learning platforms including blogs, forums especially if associated with a photograph.
- Written permission will be obtained from parents and carers before any photographs are published on the Kite Primary Federation website
- Parents should be clearly informed of the school policy on image taking and publishing.

Social networking and personal publishing on the school learning platform

- The schools will control access to social networking sites and consider how to educate pupils in their safe use.
- The schools will encourage parents to support their children when setting up a social networking profile and offer help and guidance. This includes encouraging families to follow the terms and conditions specifying the appropriate age for using sites.
- Pupils will be advised never to give out personal details which may identify them or their location.

Managing filtering

- The schools will work with the County Council and their IT consultant to ensure systems to protect pupils are reviewed and improved.
- Any unsuitable on-line material should be reported to the E-Safety coordinator
- Regular checks will be made to ensure the filtering methods are appropriate, effective and reasonable.
- A log will be kept and used to identify patterns and behaviours and therefore inform policy and educational interventions.

Skyping

- Skyping will be appropriately supervised for the pupils' age.
- Pupils will always ask permission from the supervising teacher before making or receiving a Skype call.
- Skyping will use the educational broadband network to ensure quality of service and security.

Class Dojo

- Photographs that include children will be selected carefully to be added to the child's personal story or class story depending on permissions.
- Parents are asked if they want to link to their child's account so they see what is happening inside our classrooms and schools and so children can share their learning at home.
- Promises Class Dojo make :

  - We don't share any of your information or students' information with advertisers or marketers.
  - We don't own anything you add to ClassDojo: you do.
  - Students' portfolios are private to the classroom.
  - We use the latest security best practices to protect you at all times.
  - We are compliant with COPPA, FERPA, and GDPR in Europe.
  - We will notify you if we make any changes to our practices

Managing emerging technologies

- The school will examine emerging technologies for their educational benefit and carry out a risk assessment before use in school.
- Mobile phones and associated cameras will not be used in lessons or formal school time or during an educational activity.
- Care will be taken with the use of hand held technologies in school which may not have the level of filtering required.
- Staff will use a school phone where contact with pupils and their families are required unless in an emergency.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018

Policy decisions authorising internet access

- All staff must read and sign the 'staff code of conduct' before using any schools ICT resource
- The schools will maintain a current record of all staff and pupils who are given access to school IT systems
- Parents will be asked to sign and return a consent form
- At Key Stage 1, access to the internet will be by adult demonstration with directly supervised access to specific on-line materials or by small group research closely monitored by an adult.

- Any person not directly employed by the schools will be asked to sign an 'acceptable use of schools ICT resources' before being allowed to access the internet from the schools site

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material; however it is not possible to guarantee that unsuitable material will never appear on a school computer.
- The school will monitor ICT use to establish if the E-Safety policy is appropriate and effective.

Handling E-Safety complaints

- Complaints of internet misuse will be dealt with by the senior leadership team.
- Complaints of misuse by staff will be referred to the Head teacher
- Any complaints of a child protection nature must be dealt with in accordance to child protection procedures.
- Pupils and parents will be informed of the consequences and sanctions for pupils misusing the internet and this will be in line with the schools behaviour policy.

Community use of the internet

All use of the schools internet connection by community and other organisations shall be in accordance with the E-Safety policy.

Communicating the policy - Pupils

- Appropriate elements of the e-safety policy will be shared with pupils
- E-safety rules will be posted in all networked rooms
- Pupils will be informed that network and internet use will be monitored.
- Age appropriate curriculum opportunities will be used to ensure all pupils gain an awareness of e-safety. These will be addressed on a regular basis and modified as newer risks are identified.

Staff

- All staff will read the E-Safety policy and required to sign to acknowledge that they have read and understood the policy and agree to work within the guidelines.
- Staff should be aware that the system is monitored and that professional standards are expected.
- Staff monitoring the system will be supervised by senior management and have a clear procedure for reporting

Parents

- Parents will be notified of the policy in the school brochures and on the Federation website
- All parents will be asked to sign the parent/pupil agreement when they register their children.

- Parents will be offered e-safety training to encourage them to support and encourage positive online activities with their children and help them to use the internet safely.

On The Kite Primary Federation website under the Wellbeing and E- safety page there are links to different websites which provide further E- safety advice and support.

This E-safety policy was revised by:

It was approved by the Governors on:

Review date : September 2020