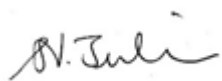


# King's Cliffe Endowed Primary School

## Online Safety Policy

**Policy Agreed** – 15<sup>th</sup> May 2023

**Review Date** – May 2024



Chair of Governors:

(signed)



### Aims

This policy aims to give an understanding of the benefits and pitfalls in the use of Computing, including internet and internet-based technologies by all users – staff, pupils and parents. It provides some guidelines as to the type of use that is unacceptable and should be avoided and describes the measures that are taken within the school to assist in the development of a safer user environment.

### Requirements

As part of the Every Child Matters agenda set out by the government, the Education Act 2004 and the Pupils' Act, it is the duty of schools to ensure that pupils and young people are protected from potential harm both within and beyond the school environment. Therefore, the involvement of pupils, young people and parents / carers is vital to the successful use of online technologies. This policy aims to explain how parents / carers, pupils or young people, can be a part of these safeguarding procedures. It also explains how pupils and young people are educated to be safe and responsible users capable of making good judgements about what they see, find and use. The term 'online safety' is used to encompass the safe use of all technologies in order to protect pupils, young people and adults from potential and known risks.

### School Networks

The school has a network that connects all computers, used by both staff and pupils, to each other and to the internet via a gateway. The staff computers are segregated from the pupil computers by using a different IP address subnet. The network is maintained by a third-party L.A. approved contractor.

All configuration and administrative information is held by them. Internet access is provided via the

L.A. approved service – the East Midlands Broadband Consortium (EMBC), whose services include accredited anti-virus, spam filtering and content filtering.

## **Pupils**

### Common Risks to Pupils

Potential risks to pupils can generally be placed into four groups referred to as the Four C's. These are Content, Contact, Conduct and Commerce. These are identified in Keeping Children Safe In Education (2021) and are defined below;

- **Content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, anti-Semitism, radicalization and extremism
- **Contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and/or financial scams

Through the Pupils' Online safety Policy and the Computing curriculum, the school aims to increase pupils' awareness and understanding of such risks and teach them the safest and most appropriate ways in which to respond.

### Pupils' Online Safety Policy

The Pupils' Online Safety Policy has been produced as an easy-to-understand booklet, a copy of which is given to each pupil when they first start using the computers at the school. Posters are also positioned near to computers to remind the pupils of key considerations when using the internet. The policy booklet is reviewed and updated each year by the school council and through whole school assemblies. This ensures that pupils' understanding grows and develops as they move through the school and that they take ownership of it. The policy is also shared with parents annually at the beginning of each new school year and revisited termly in classes as part of the

Computing curriculum. All class teachers have access to suitable and age-appropriate resources from EYFS through to Upper KS2. In conjunction with this, an Online Safety Contract is written, agreed upon and signed by each member in the class. This ensures that children have a clear understanding of how they are expected to use the internet safely in class and all know how to conduct themselves online.

### The Online Safety Curriculum

Teachers follow the learning objectives outlined in the national curriculum when planning and delivering the Computing curriculum, of which there are specific objectives addressing online within each year group. The Computing curriculum is supplemented by Teach Computing by NCCE, as well as the Espresso Coding by Discovery Education, both of which highlight Online safety considerations for teachers and/or pupils in their plans. Online safety is specifically addressed by using the Education for a Connected World framework with differentiated statements across the key stages. Online safety is revisited each term by all classes.

### Home Use

Whilst the school does not aim to control use of the internet at home, pupils will be encouraged to develop an attitude towards the internet and other forms of electronic communication that supports the aims of the school online safety policy as described in the pupils' Online Safety Policy booklet. Parents will be encouraged to consider the potential for unmonitored internet usage at home and the various mechanisms that can be employed to ensure that their children have a safe and rich experience of using the internet.

### Incident Reporting

Where incidents of inappropriate internet, email or social networking use occur, pupils will be encouraged to discuss their experiences with a teacher and/or their parents. Additional coaching within the class will be employed to make pupils more aware of what to avoid on the internet, along with discussion with the pupil's parents about appropriate online safety strategies for use both at school and at home. Where necessary, recurrences of such incidents will be dealt with through the school's safeguarding policy. All incidents are to be reported using the CPOMS format as Cause for Concern -> E-Safety. ICT lead is to be notified immediately to address any issues and report findings to the relevant persons.

## **Staff**

### Staff Internet and Email Use

Use of the internet and email by members of staff is permitted and encouraged where such use supports the goals and objectives of the school.

However, the school has a policy for the use of the internet and email whereby staff must ensure that they comply with current legislation use the Internet/email in an acceptable way.

### Unacceptable Internet Use

The following is deemed unacceptable internet use or behaviour by staff:

- visiting internet sites that contain obscene, hateful or pornographic material
- using the computer to perpetrate any form of fraud, or software, music or video piracy
- using the internet to send offensive or harassing material to other users
- downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such license
- hacking into unauthorised areas
- creating or transmitting defamatory material
- undertaking deliberate activities that waste staff effort or networked resources
- introducing any form of computer virus into the school network

### Unacceptable Email Use

The following is deemed unacceptable email use or behaviour by staff:

- use of school communications systems to set up personal businesses or send chain letters
- distributing, disseminating or storing images, text or materials that might be considered indecent, pornographic, obscene or illegal
- distributing, disseminating or storing images, text or materials that might be considered offensive or abusive, in that the context is a personal attack, sexist or racist
- accessing copyrighted information in a way that violates the copyright
- breaking into the system or unauthorised use of a password / mailbox

- broadcasting unsolicited personal views on social, political, religious or other non-school related matters
- transmitting unsolicited commercial or advertising material

### Monitoring

The school accepts that the internet and email are valuable tools with which staff may research, communicate and plan. However, misuse can have a negative impact upon staff productivity, the development of pupils and the reputation of the establishment. The use of the internet within the classroom is encouraged, but staff should test all activity before use with pupils. This is to avoid any embarrassment and avoidable exposure of the pupils to unsuitable material.

All of the school's internet and email resources are provided for school purposes. Therefore, the school maintains the right to monitor the volume of internet and network traffic, together with the internet sites visited, and to examine any email systems and data recorded within. The specific content of any transactions will not be monitored unless there is a suspicion of improper use.

In order to ensure compliance with this policy, the school also reserves the right to use monitoring software. Such monitoring is for legitimate purposes only and will be undertaken in accordance with a procedure agreed with staff.

### Sanctions

Failure to comply with these guidelines will result in sanctions ranging from disciplinary procedures such as verbal and written warnings, through to dismissal.

### Social Networking

Many people, including members of staff, parents and some pupils, will be members of social networking site. Through the school's Online Safety Policy and Computing lessons, pupils will be made aware of the dangers of social networking sites and those that are inappropriate for their age. These facilities will not be made available through school, and it will not be permitted for pupils to access social networking sites from school equipment. Parents will be advised of the desirability of monitoring their children's use of social networking. Should it be suspected that a child has been using social networking in an ill-advised manner, this will be dealt with through the school's usual child protection procedures.

Staff use of social networking is not prohibited; however, staff are reminded of their duty of professional conduct when communicating with other members of the profession and are advised against all contact with parents and pupils through social networking.

#### Staff Use of Personal Computing Resources

It is accepted that staff may utilise their own Computing resources to help them undertake their role within the school. This could range from using a personal home computer to prepare lessons to using personal equipment within lessons. It is not normally desirable, or encouraged, for anyone to connect their own personal equipment to the school network.

#### Storage of Data

Storage of data pertaining to individuals (either pupils or members of staff) on non-school equipment is strongly discouraged. To ensure data protection and confidentiality, such data should only be stored on school equipment that is encrypted and/or password protected. Any portable storage systems must be encrypted and/or password protected.

#### Prevention of Virus Transmission

Members of staff should ensure that their personal Computing equipment is loaded with appropriate virus protection software and that this is regularly updated. Use of anti-virus software is essential in the protection of both personal and school Computing equipment.

#### Transferring Data Between Personal & School Equipment

It is often necessary to transfer materials between personal and school equipment. Where possible, staff are encouraged to use internet-based methods – such as e-mail, WeTransfer, OneDrive or the Teams platform. This ensures that security and virus checking procedures can be applied without further measures. It is accepted that there are circumstances in which it is more suitable to use some form of removable media device (such as a writable CD/DVD or memory-stick). When using a removable media device, it is imperative that the device is virus checked, encrypted and password protected. These devices are known to be one of the greatest causes of uncontrolled virus transmittal, and through their potential loss, they pose the greatest risk to security and breaches of data protection.

### Attaching Personal Equipment to School Resources

On occasions, a member of staff may wish to attach personal equipment to the Computing resources within the school (e.g. a camera, electronic microscope, or other such devices). Before such actions are taken, the member of staff is encouraged to verify any issues of compatibility with the school equipment. It also should be remembered that there are often licensing restrictions associated with software which may have to be loaded to support the peripheral device being connected. It is recommended that the Computing coordinator is informed of the equipment to be connected and any support software to be loaded. Staff are warned that should any compatibility issues arise which cause malfunctioning (of software or hardware), this may result in the school having to contact their support service provider – notwithstanding the inconvenience which will result in the loss of use of the computer until the issue is rectified.

### **Use of Other Electronic Information & Communication Equipment**

#### Mobile Telephones

Pupils are not permitted to have mobile telephones on the school premises. Should a parent wish their child to have a telephone at school, this will only be permitted through prior agreement with the Head Teacher, and under exceptional circumstances. Mobile phones belonging to children are to be kept in the school office until the end of the day, when the child collects them on their way out.

Members of staff are requested not to use mobile telephones within the pupil areas, and when not in use, store them in a secure location with the ringtone on silent. It will not be permissible for an individual's mobile telephone to connect to the school network services.

#### Smart Watches

Increasingly, pupils and staff are wearing smart watches on the school premises. Whilst school does encourage the healthy lifestyle that these devices often promote, we recognise that these devices can and are often used for communication purposes. Smart watches should be set to 'Do Not Disturb' mode or one similar to disable the communication elements of the devices. These devices should also be set to silent whilst on school premises.



## Home Learning

Due to the recent COVID-19 outbreak, teachers have been forced to communicate with their classes through the use of Zoom, FaceTime and Teams. Whilst staff have adapted quickly to the changes this brings, it is necessary for staff to follow procedures to ensure the safety of children and themselves.

All remote learning is to take place using Teams as a host. Staff and children have their own accounts that are to be used. Classes may use Tapestry to send out notices and work, but all remote video calling should be done via Teams.

Staff and pupils are to use appropriate screen names when partaking in online learning. This is so that participants are clearly identifiable throughout the meeting and allows staff to accurately make use of the waiting room admittance at the start of each session.

The chat feature settings must be changed so that children cannot send private messages to each other during the session. This is to prevent any harm from inappropriate messages between pupils as the host cannot read these. The chat feature should be entirely disabled or at least the option to send private messages removed. Staff should consider the surroundings in which they are hosting their meetings. The background should be relatively empty and free from any items which could breach the privacy of the host or reveal any personal data about the host or students e.g. data sheets in the background. Staff should make use of the virtual or blurred background features on the video call software. This applies to children too as they should be in an appropriate environment for their learning.

When inviting participants to meetings, meeting details must not be shared on social media.

Meeting IDs should be automatically generated and passwords must be set to allow entry. These passwords must be secure, containing upper and lower-case letters, numbers and symbols.

Any 1-1 meetings with children must be recorded for safeguarding purposes, especially if a third party is not in the immediate vicinity.

## Review

This policy will be reviewed on an annual basis, or at an earlier interval should it be found that advancements in on-line and electronic communications technologies dictate this. This policy should be read in conjunction with the Child Protection/Safeguarding Policy.

