King's Cliffe Endowed Primary School

Online Safety Policy

Policy Agreed – 4th September 2025

Review Date – July 2026

Chair of Governors: Mr Lee O'Connor (signed) 

Policy 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.

School Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

Requirements

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. In order to keep children safe online, this policy is based upon the Department for Education's (DfE's) statutory safeguarding guidance, Keeping children Safe in Education, and its advice for school on;

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

The involvement of pupils, young people and parents / carers is vital to the successful and safe 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.

Roles and responsibilities

The Governing Board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix A)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

<u>The Headteacher</u>

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

<u>The Designated Safeguarding Lead (DSL)</u>

Details of the school's designated safeguarding lead (DSL) and deputy designated safeguarding lead (DDSL) are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

<u>The ICT Manager</u>

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material

- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

Staff and Volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix A), and ensuring that pupils follow the school's terms on acceptable use (appendix B)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing contacting the DSL. Queries and support with filtering and monitoring can be found from contacting Securely.
- Following the correct procedures by making note in the IT book found in the school office. Any requests made in the IT book will be shared with Securely who will make changes to the filtering and monitoring system for example; if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix B)

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix A).

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 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 a DfE approved provider; EXA Broadband and the filtering and monitoring systems are provided by Securely. Our IT systems are overseen and managed by EasiPC.

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.

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as 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, such as 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; and
- **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 displayed throughout the school to support them with how to stay safe online. 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 The National Centre for Computing Education - www.teachcomputing.org and progressive online safety lesson planning is readily available for staff to access via Teams. Online safety is specifically addressed by using the Education for a Connected World framework with differentiated statements across the key stages Education for a Connected World (publishing.service.gov.uk). Online safety is revisited every term by all classes.

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly

- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, all pupils will know:

- That people sometimes behave differently online, including pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

<u>Home Use</u>

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.

To help parents/carers with supporting their child with how to be safe online at home. We educate parents/carers about online safety, sharing helpful tips and information that can be used with their child. Monthly communications to parents share up to date and relevant information about online safety using The National College as the source of reliable and current Online Safety information.

Our school also raises parents/carers' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents/carers.

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

Cyber-bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power.

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their pupils relevant to their age and understanding.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

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 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.

Examining Electronic Devices

The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher/DSL/DDSL
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the headteacher, DSL and DDSL to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Artificial Intelligence (AI)

The use of Artificial Intelligence (AI) systems at KCEPS
Risk assessment for the use of AI and an AI specific Staff Acceptable Use Agreement can be found in appendices.

As Generative Artificial Intelligence (gen AI) continues to advance and influence the world we live in , its role in education is also evolving. There are currently 3 key dimensions of AI use in schools: learner support, teacher support and school operations; ensuring all use is safe, ethical and responsible is essential.

At KCEPS, we realise that there are risks involved in the use of Gen AI services, but that these can be mitigated through our existing policies and procedures.

Staff and learners will be educated about the safe and ethical use of AI, preparing them for a future in which these technologies are likely to play an increasing role.

The safeguarding of staff and learners will, as always, be at the forefront of our policy and practice.

- KCEPS acknowledges the potential benefits of the use of AI in an educational context - including enhancing learning and teaching, improving outcomes, improving administrative processes, reducing workload and preparing staff and learners for a future in which AI technology will be an integral part. Staff are encouraged to use AI based tools to support their work where appropriate, within the frameworks provided below and are required to be professionally responsible and accountable for this area of their work.
- All staff will comply with all relevant legislation and guidance, with reference to guidance contained in Keeping Children Safe in Education and UK GDPR
- KCEPS will provide relevant training for staff and governors in the advantages, use of and potential risks of AI. We will support staff in identifying training and development needs to enable relevant opportunities.
- Learning about AI will be embedded as appropriate in our curriculum offer, including supporting learners to understand how gen AI works, its potential benefits, risks, and ethical and social impacts. KCEPS recognises the importance of equipping learners with the knowledge, skills and strategies to engage responsibly with AI tools at an age-appropriate level.
- As set out in the staff acceptable use agreement (appendix D) staff will be supported to use AI tools responsibly, ensuring the protection of both personal and sensitive data. Staff should only input anonymised data to avoid the exposure of personally identifiable or sensitive information.
- Staff will always ensure AI tools used comply with UK GDPR and other data protection regulations. They must verify that tools meet data security standards before using them for work related to the school.
- Only those AI technologies approved by the school may be used. Staff should always use school-provided AI accounts for work purposes. These accounts are configured to comply with organisational security and oversight requirements, reducing the risk of data breaches.
- We will protect sensitive information. Staff must not input sensitive information, such as internal documents or strategic plans, into third-party AI tools unless

explicitly vetted for that purpose. They must always recognise and safeguard sensitive data.

- KCEPS will ensure that when AI is used, it will not infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the learners, being used to train generative AI models without appropriate consent.
- AI incidents must be reported promptly. Staff must report any incidents involving AI misuse, data breaches, or inappropriate outputs immediately to the relevant internal teams. Quick reporting helps mitigate risks and facilitates a prompt response.
- We are aware of the potential risk for discrimination and bias in the outputs from AI tools and have in place interventions and protocols to deal with any issues that may arise. When procuring and implementing AI systems, we will follow due care and diligence to prioritise fairness and safety.
- The school will support parents and carers in their understanding of the use of AI in the school sharing information and resources provided by The National College.
- We will prioritise human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans and critically evaluate AI-generated outputs. They must ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing. This is especially important for external communication to avoid spreading misinformation.
- Recourse for improper use and disciplinary procedures. Improper use of AI tools, including breaches of data protection standards, misuse of sensitive information, or failure to adhere to this agreement, will be subject to disciplinary action as defined in Staff Disciplinary Policy.

Staff

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse

- Children can abuse their peers online through:

  -Abusive, threatening, harassing and misogynistic messages

  -Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups

  -Sharing of abusive images and pornography, to those who don't want to receive such content

- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks

The DSL and DDSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

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 and 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

Filtering and 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. When children have access to a computing device they must login using their unique username and password. This allows members of staff to monitor in real time what the children have access to using the Securely filtering and monitoring program. Staff members are alerted of anything that may be of concern.

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 individuals' 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 previous COVID-19 outbreaks, 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.

Appendix A

Acceptable Use Staff Policy

This policy helps adults and the pupils at King's Cliffe Endowed Primary School stay safe when using electronic equipment and the internet.

You must read this policy in conjunction with the Online Safety Policy and Safer Working Practice Guidance. Once you have read and understood both you must sign this policy sheet.

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), you must not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way that could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share your password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking parent permission has been given
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data you are not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

- **Guidance for Safer Working Practice** is to be adhered to by all staff in their professional duties when in school and when in communication with pupils and their families.

- **Social Networking** is allowed in school under accordance with the E-Safety Policy. Staff using social networking for personal use should never undermine the school, staff, parents, or pupils. Staff should not become 'friends' with parents or pupils on personal social networks. However, we recognise this may be difficult if you are a TA living in the village and have parent 'friends.' If this is the case, you should always adhere to

confidentiality and not do or say anything that will bring the school, pupils, staff or parents into disrepute.

- **Use of email**- staff are not permitted to use school email address for personal business. All email should be kept professional. Staff are reminded that school data, including emails, is open to Subject Access requests under the Freedom of Information Act.

- **Passwords-** staff should keep passwords private. There is no occasion when a password needs to be shared with another member of staff or student or IT support.

- **Data Protection-** If it is necessary for you to take work home, or off site, you should ensure that your device (laptop or Ipad) is encrypted. On no occasion should data concerning personal information be taken offsite on an unencrypted device.

- **Images and Videos** should not be uploaded onto any internet site or service images or videos of yourself, other staff, or pupils without consent. This is applicable professionally (in school) or personally (i.e. staff outings).

- **Use of a Personal Mobile Phone** is not permitted during school hours in any part of the school grounds other than in the staff room at break time and lunchtime. Mobile phones should be stored out of sight and silent/turned off. If you are waiting for an urgent call this must go through the school office. Children must not see staff walking through school or on the playground with a mobile telephone.

- **Use of a Smart Watch** is not permitted during school hours in any part of the school grounds other than in the staff room at break time and lunchtime. 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 understand 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.

- **Use of Personal ICT** is not permitted during school hours in any part of the school grounds. There should not be a need to bring a personal laptop or I-pad into school; however, if an I-pad is used for personal communication instead of a mobile phone, this can only be used in the staff room at break time and lunch time during school hours.

- **Viruses and other Malware**- any virus outbreaks are to be reported to the E-Safety officer as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the school.

- **E-Safety-** like health and safety, e-safety is the responsibility of everyone. As such you will promote positive messages in all use of ICT whether you are with other members of staff or with pupils.

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material that might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly and ensure that pupils in my care do so too.

Name:…….

Signed ……..Date: ……

Appendix B

Pupil E-Safety Agreement

These rules help me to stay safe when using the laptops/I-Pads, my mobile phone or smart watch. **I agree that:** (pupils tick each box and sign their names)

- ☐ On all the laptops/I-Pads I will use the correct username and password to log in
- ☐ I will not use other people's work/pictures without permission
- ☐ I will only use the internet when an adult is in class with me, and I will ask permission before entering any website, unless my teacher has already told me that site is allowed
- ☐ I will not take pictures of anyone without their permission
- ☐ If I see anything I am unhappy with, or feel uncomfortable about, I will tell a teacher immediately, or my parents if I am at home.
- ☐ I will only send polite, sensible messages and will never share personal information, or arrange to meet someone
- ☐ I will not open e-mails from strangers.
- ☐ I understand that some people on the internet are not who they say they are, and some people can be hurtful. I will tell my teacher if I am ever concerned in school, or my parents if I am at home.
- ☐ I will not bring my mobile phone to school. The only exception is if I am a Year 5 or 6 pupil who walks to and from school without my parent(s)/carer(s). If I have my parent(s)/carer(s) permission, I have the option of bringing my mobile phone, which must be handed into the school office on my arrival and collected from the school office at the end of the day.
- ☐ If I wear a smart watch to school this must only be used as an analogue/digital watch and switched to DO NOT DISTURB whilst I am at school.
- ☐ I understand that if I deliberately break these rules, I will be stopped from using the internet, or have my phone/smart watch confiscated. I will be spoken to by my teacher, or the Head Teacher and my parent(s)/carer(s) will be informed.

Signed (Pupil): ……
Signed (Parent(s)/Carer(s))……
Date: ……

Appendix C

Use of AI Tools Risk Assessment

Risk Area	Risk Description	Mitigation Measures
Data Protection and Privacy Breaches	Unauthorised access to sensitive data or personal information, leading to safeguarding concerns and commercial risk.	Implement strong encryption, regular audits, and GDPR-compliant data management policies and conduct regular privacy audits.
Cyberbullying	Increased potential for bullying through AI-mediated communication tools.	Monitor AI communication tools, implement clear reporting mechanisms, and provide student support.
Over-reliance on AI	Over-reliance on AI tools reducing interpersonal interactions among students. Reduction in teacher autonomy and critical decision-making by overusing AI tools.	Encourage collaborative learning activities and balance AI use with social engagement. Define clear boundaries for AI use and regularly review its impact on pedagogy.
Emotional Manipulation	AI systems unintentionally affecting student mental health through curated content.	Monitor AI-generated content, involve mental health professionals, and promote media literacy.
Inappropriate Content or Conduct	AI exposing learners to harmful or unsuitable materials / behaviour	Conduct rigorous testing of AI tools, apply effective filtering and monitoring and ensure human oversight.
Mental Health Impacts	Overuse of AI tools causing stress, anxiety, or dependency in learners.	Monitor usage patterns, provide mental health resources, and set expectations on use of AI systems.
Bias and Discrimination	AI systems propagating biases that impact student wellbeing or	Regularly audit AI algorithms for bias and provide inclusive

	inclusion. AI models producing discriminatory or biased outcomes.	media literacy education and training.
Misuse of AI	Learners using AI tools for harmful, unethical or illegal purposes (e.g. nudification).	Educate learners on responsible and appropriate AI use and establish clear usage policies.
Misinformation	Creation or spread of harmful or misleading AI-generated content.	Educate staff and learners to verify AI outputs and establish clear policies for verifying content authenticity.
AI Ethics Awareness	Lack of awareness among staff and learners about ethical implications of AI.	Provide training and education on AI ethics and its responsible usage. Establish an 'Ethics in AI' group.
Data Accuracy	AI systems generating inaccurate or misleading recommendations.	Regularly validate AI outputs and involve human oversight in decision-making.
Legal Compliance	Non-compliance with laws regarding AI usage and learner data.	Understand legal requirements. Conduct legal reviews and consult experts on AI-related regulations.
Cyber-Security	Increased use of AI tools in cyberattacks targeting school systems and data.	Strengthen cybersecurity protocols and educate staff and learners on safe online practices.

Appendix D

Staff Use of AI Acceptable Use Agreement

Emerging technologies, including Artificial Intelligence (AI), are increasingly integrated into educational settings and the lives of staff and learners. These technologies have immense potential to enhance creativity, promote personalised learning, and improve operational efficiency. However, their use also presents risks that require clear policies and practices to ensure safety, security, and ethical application.

This acceptable use policy aims to ensure:

- Staff and volunteers are responsible users of AI and emerging technologies, prioritising safety and ethical considerations.
- School systems and users are protected from misuse or harm resulting from the use of AI.
- Staff have a clear understanding of their responsibilities when engaging with AI and emerging technologies in professional and personal contexts.

Acceptable Use Policy Agreement

I understand that I must use AI and emerging technologies responsibly to minimise the risk to the safety, privacy, or security of the school community and its systems. I acknowledge the potential of these technologies for enhancing learning and will endeavour to integrate them in a way that aligns with the school's policy, ethos and values.

For my professional and personal safety:

- I understand that the school will monitor my use of AI tools and technologies.
- I will only use AI tools and technologies for purposes authorised by the school and will ensure compliance with data protection laws (e.g. UK GDPR) when handling personal data.
- I will ensure that any sensitive or personally identifiable information about staff, students, or parents/carers are not inputted into AI systems
- I will only use AI tools that have robust security measures in place.
- I will report any AI-related incidents or anomalies that could indicate misuse, bias, or harm to the appropriate person immediately.

In my communications and actions:

- I will respect copyright, intellectual property, and ethical standards when uploading content to prompt AI output.
- I will critically evaluate the outputs of AI systems to avoid spreading misinformation or biased content and will ensure that all AI-assisted decisions are made with appropriate human oversight.
- I will communicate professionally and responsibly when using AI systems.
- I will ensure transparency through appropriate attribution where AI has been used.

When engaging with learners:

- I will educate learners on the safe, ethical, appropriate and effective use of AI and ensure that children abide by the age ratings of AI tools.
- I will use AI tools to engage with learners in ways that uphold and enhance their privacy, wellbeing, and trust.

When using the school's systems and resources:

- I will use AI systems in compliance with established security measures and access protocols.
- I will ensure that any AI applications used in teaching or administration are vetted and comply with the school's policies.
- I will ensure generative AI tools are not used to impersonate others or create deceptive or harmful content.

When handling data:

- I will ensure compliance with the school's data protection policies when using AI for data analysis or reporting.

Responsibility and Accountability:

- I will use generative AI tools responsibly to create authentic and beneficial content, ensuring respect for individuals' identities and well-being.
- I understand that misuse of AI or emerging technologies could lead to disciplinary actions, including warnings, suspension, or referral to the appropriate authorities.
- I acknowledge that this agreement applies to all AI-related activities within and outside of school premises that are connected to my professional responsibilities.

Name:.....

Signed .....**Date:** .....