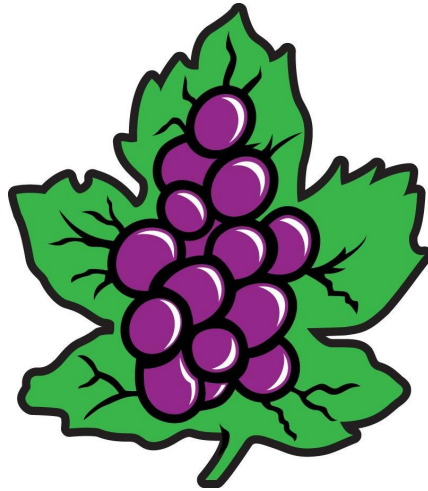


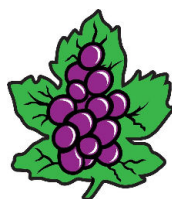


E-SAFETY POLICY

Kerem School

Approved by: Safeguarding and Wellbeing Committee **Written:** September 2021

Last reviewed on: August 2026 **Next review due:** August 2027



KEREM SCHOOL

(This policy also applies to the Early Years Foundation Stage)

E-Safety Policy

Kerem School believes that the potential technology has to impact the lives of all citizens increases year on year. In many areas, technology is transforming the way that schools teach and how children learn. At home, technology is changing the way children live and the activities in which they choose to partake; these trends are set to continue.

While developing technology brings many opportunities, it also brings risks and potential dangers, of which these are just a few:

Access to illegal, harmful or inappropriate images or other content

Access to misinformation, disinformation or conspiracy theories

Unauthorised access to, loss of or sharing of personal information

The risk of being subject to grooming by those with whom they make contact on the internet.

The sharing/distribution of personal images without an individual's consent or knowledge

Inappropriate communication/contact with others, including strangers

Cyber-bullying

Access to unsuitable videos/internet games

An inability to evaluate the quality, accuracy and relevance of information on the internet

Plagiarism and copyright infringement

Illegal downloading of music or video files

The potential for excessive use, which may impact social and emotional development and learning.

This policy sets out how we strive to keep children safe with technology while they are in school. We recognise that children are often more at risk when using technology at home, where we have no control, but rely on parents to have structures in place to keep their children safe. This policy also sets out how we work to educate children about the potential risks. It is important that schools, as well as parents, adopt strategies to assist in this process.

Policy and Leadership

Kerem School believes that good planning and management that recognises the risks will help to ensure appropriate, effective, safe pupil use. Below are the key people responsible for developing our E-Safety Policy and keeping everyone safe within ICT.

Responsibilities: ICT/Computing Lead

Our Computing Lead is the person responsible to the Head Teacher and Governors for the day-to-day issues relating to e-safety. Where there is no Computing Lead, this role will be taken on by the DSL in close liaison with Nippy Gecko, our external ICT technician.

The Computing Lead:

- Takes day-to-day responsibility for e-safety issues and has a leading role in establishing and reviewing the school's e-safety policies/documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident
- Provides advice for staff
- Liaises with school ICT technical staff
- Receives appropriate training and support to fulfil their role effectively
- Has responsibility for blocking / unblocking internet sites in the school's filtering system / passing on requests for blocking/unblocking to the IT technician, Nippy Gecko.
- Has responsibility for changing the Internet access password at least once a term.
- Ensuring that the children are taught both by the ICT teacher and other staff about e-safety.
- Liaises with the DSL to ensure that sufficient filtering and monitoring systems are in place at the schools (**KCSIE 2026**)
-

Responsibilities: Head Teacher/DSL

- The Head Teacher, together with the DSL are responsible for ensuring the safety (including e-safety) of members of the school community, though the day-to-day responsibility for e-safety is delegated to the Computing Lead
- The Head Teacher and the DSL should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

Responsibilities: Classroom-Based Staff

Teaching and Support Staff are responsible for ensuring that:

- They have an up-to-date awareness of e-safety matters and the current school e-safety policy and practices
- They have read, understood and signed the School's Acceptable Use Policy for Staff
- They report any suspected misuse or problem to the E-Safety Coordinator
- Digital communications with students, email, should be on a professional level and only carried out using official school systems
- E-safety issues are embedded in the curriculum and other school activities.
- Websites and videos used in the classroom should be age-appropriate and handled with caution.
- They are careful when inputting the access password to ensure that children cannot see what they are typing
- They report any breach of the access password to the DSL and Computing Lead immediately

Responsibilities: ICT Technician - Nippy Gecko

The ICT Technician is responsible for ensuring that:

- The school's ICT infrastructure is secure and is not open to misuse or malicious attack
- Users may only access the school's networks through a properly enforced password protection policy
- Shortcomings in the infrastructure are reported to the Computing Lead, Head Teacher and/or DSL so that appropriate action may be taken

Policy Scope

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

The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the School.

The School will deal with such incidents and associated behaviour falling within this policy as well as relating to the anti-bullying policies, and will, where known, inform parents/ carers of incidents of inappropriate e-safety behaviour that take place in and out of school.

Acceptable Use Policies (AUP) / Rules for Responsible ICT Use

All members of the School community are responsible for using the School ICT systems in accordance with the appropriate acceptable use policy, which they will be expected to sign before being given access to School systems.

Acceptable use policies are provided in Appendix 1 of this policy for:

- Pupils (EYFS / KS1 / KS2)
- Staff (and volunteers)

Acceptable use policies are revisited and re-signed annually at the start of each school year. These are amended in light of new developments and discussions with the children, which take place at that time. Copies are sent home for further discussion with parents.

For children in the EYFS and KS1, parents may sign on behalf of their children.

Staff and volunteers sign when they take up their role in school and again, in the future, if significant changes are made to the policy.

Parents sign once when their child enters the school. The parents' policy also includes permission for use of their child's image (still or moving) by the school, permission for their child to use the school's ICT resources (including the internet) and permission to publish their work. A copy of the pupil AUP is made available to parents at this stage and at the beginning of each year.

Community users sign when they first request access to the school's ICT system.

Whole School approach and links to other policies

This policy has strong links to other school policies as follows:

ICT Policies:

- Computing and Communication Technology Policy - How ICT is used, managed, resourced and supported in our school
- E-Safety Policy - How we strive to ensure that all individuals in school stay safe while using ICT. The e-safety policy constitutes a part of the ICT policy.
- Internet Policy.

Other policies relating to e-safety:

- Anti-bullying – links to cyberbullying
- PSHE: E-Safety has links to this – staying safe
- Keeping Children Safe in Education(2026) - online safety

Safeguarding

Safeguarding children electronically is an important aspect of e-safety. The E-Safety Policy forms a part of the School's Safeguarding Policy.

The school deploys an ICAP web filtering server that integrates with the network and provides rich web and content filtering of internet traffic passing into the internal network. It currently enforces two types of filter policies on users, one for pupils and the other for teachers. The filter policies allow us to control access to 50 categories of websites (dating, nudity, gambling, explicit adult content, gaming and others), block resources with explicit content and block illegal or potentially malicious file downloads. The web filter is configured to record all blocked events and upload these to the reports database every hour and generate the reports daily on internet activity.

Illegal or inappropriate activities and related sanctions

The school believes that the activities listed below are inappropriate in a school context and that users should not engage in these activities when using school equipment or systems (in or out of school).

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on material, remarks, proposals or comments that contain or relate to:

- Child sexual abuse images (illegal - The Protection of Children Act 1978)
- Grooming, incitement, arrangement or facilitation of sexual acts against children (illegal – Sexual Offences Act 2003)
- Possession of extreme pornographic images (illegal – Criminal Justice and Immigration Act 2008)
- Criminally racist material in the UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) (illegal – Public Order Act 1986)
- Pornography
- Promotion of any kind of discrimination
- Promotion of racial or religious hatred
- Threatening behaviour, including promotion of physical violence or mental harm
- Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute

Additionally, the following activities are also considered unacceptable on ICT equipment provided by the school:

- Using school systems to run a private business
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Carrying out sustained or instantaneous high-volume network traffic (downloading/uploading files) that causes network congestion and hinders others in their use of the internet
- Online gambling and non-educational gaming
- Use of personal social networking sites/profiles for non-educational purposes

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (see above), it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures.

Use of handheld technology (mobile phones/ iPads/tablet devices)

We recognise that the area of mobile technology is rapidly advancing, and it is our school's policy to review its stance on such technology on a regular basis.

Currently, our policy is this:

- Members of staff are permitted to bring their personal mobile devices into school. They are free to use these devices in school, outside teaching time in the staffroom and office.
- Staff are only permitted to use their personal devices for school purposes in the case of an emergency e.g. to make a call to the emergency services or parents when a school phone is unavailable.
- If staff have their personal phones with them on a school trip, these must remain in their bags and only be used in an emergency e.g. when the Kerem phone is not working or has no reception, or is not in their possession (for example, when the class is split into groups)
- On residential trips, staff are permitted to have their personal devices, but they must only be used in their own bedrooms or areas where there are no children present.
- All teachers are provided with school iPads for use during lesson times
- Where pupils are deemed to be 'lone walkers' (walking to and/or from school independently) and parents feel it is necessary for their child to bring a phone to school, pupils are permitted to bring their personal **mobile phones** into school. These phones **cannot be smartphones** and **must** be handed in to the office each morning. Parents must fill in a permission request form before their child is allowed to carry a mobile phone.

- Children will sign in to acknowledge that they have deposited their phone before it is locked away. They will be handed back to pupils at the end of the day as they leave school. Children will sign out that they have taken them.
- Under no circumstances will children have access to their phones during the school day, and devices should not be left in pupils' bags or coats.
- Children are **not permitted to have Smartwatches** in school. Should a child bring one in, it will be treated in the same way as a phone.
- At the main school, teachers are permitted to have Smartwatches. However, they are not permitted to use them to take photographs at any time and can only use them to send emails outside teaching time in the staffroom and office.
- Teachers at the EYU are not permitted to have smartwatches at any time.
- Digital watches that only work as a step counter are permitted. However, if a step-counting watch also has the ability to be used for photos or communication, we will ask children not to wear these or to hand them to their class teacher. Should step-counting watches become a distraction, children will not be permitted to wear them. This will be considered on a case-by-case basis.

iPads:

Members of staff are given an iPad for use in school to help enhance learning.

Staff are responsible for the upkeep of the iPad. It is their responsibility if the iPad is lost, stolen or needs to be repaired due to their own negligence.

Pupils in Year 3 to Year 6 have iPads purchased by the school and claimed back through the school bill.

Parents will pay for repairs should the negligence occur, including but not limited to:

- Dropping the iPad
- Leaving the iPad on the floor/ a chair
- Carrying the iPad in a non-conventional way

Mobile phone use in the EYU

To enforce the safety and welfare of children in our care, we operate a personal mobile phone usage policy which stipulates that personal mobile phones cannot be used when in the presence of children.

- To enforce this we will ensure that:
- All mobile phones will be kept in the staff room throughout contact time with children.
- Mobile phone calls may only be taken during staff breaks or in staff members' own time.
- If you have a personal emergency you are free to use the school's phone or make a personal call from your mobile in the designated staff area of the school.
- Staff need to ensure that managers have up-to-date contact information and that staff make their families aware of emergency work telephone numbers. This is the responsibility of the individual staff member.
- During group outings nominated staff will be allowed to carry a 'Kerem' mobile phone, which doesn't allow photo or internet access, and which is to be used for emergency purposes only.

- The Early Years Lead is able to use her school mobile phone for emergencies and for communicating with the main school.

Use of communication technologies

Email

Access to email is provided for all users in school via a Google system accessible via the web browser (Google Chrome) from their desktop. These official school email services may be regarded as safe and secure and are monitored.

- Staff and pupils should use only the school email services to communicate with others when in school
- Users need to be aware that email communications may be monitored
- Pupils have access to an individual email account for communication within school.
- A structured education programme is delivered to pupils which helps them to be aware of the dangers of and good practices associated with the use of email.
- Staff may only access personal email accounts on school systems for emergency or extraordinary purposes (these may be blocked by filtering).
- Users must immediately report to their class teacher/e-safety coordinator – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

Use of digital and video images

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Members of staff are allowed to take digital still and video images to support educational aims but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be captured using school equipment; the personal equipment of staff should not be used for such purposes if the images are to be retained on the device e.g. iPads. Images should be uploaded onto the school system and the images deleted from the device.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission

Use of web-based publication tools

Our school uses the public-facing website, www.keremschool.co.uk, for sharing information with the community beyond our school. This includes, from time to time, celebrating work and achievements of children.

All users are required to consider good practice when publishing content.

- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff (never pupils).

- Only pupils' first names are used on the website, and only then when necessary.
- Detailed calendars are not published on the school website.
- Photographs published on the website, or elsewhere, that include pupils will be selected carefully and will comply with the following good practice guidance on the use of such images:
- Pupils' full names will not be used anywhere on a website or blog, and never in association with photographs
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Professional standards for staff communication

- In all aspects of their work in our school, teachers abide by the Teachers' Standards as described by the DfE
(<http://media.education.gov.uk/assets/files/pdf/t/teachers%20standards.pdf>). Teachers translate these standards appropriately for all matters relating to e-safety.
- Any digital communication between staff and pupils or parents/carers (email) must be professional in tone and content.
- These communications may only take place on official (monitored) school systems.
- Personal email addresses, text messaging or public chat / social networking technology must not be used for these communications.
- Staff constantly monitor and evaluate developing technologies, balancing risks and benefits, and consider how appropriate these are for learning and teaching. These evaluations help inform policy and develop practice.

E-safety education

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience. This is particularly important for helping children to stay safe outside of school, where technical support and filtering may not be available to them.

E-safety education will be provided in the following ways:

- A planned e-safety programme should be provided as part of ICT, PHSE and other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school.
- Outside speakers will be invited to provide added education for KS2 and teachers will include e-safety as part of the RSHE curriculum.
- All parents are invited to a talk on e-safety.
- Key e-safety messages should be reinforced through further input via assemblies and pastoral activities, as well as informal conversations when the opportunity arises.
- Pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT both within and outside school.

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

Raising awareness of e-safety:

Staff

Safeguarding professional development for staff includes aspects of online safety so staff are fully informed and up to date on the safeguarding risks children may face online.

Parents and carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and the monitoring and regulation of their children's online experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet, and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

The school will therefore seek to provide information and awareness to staff, parents and carers through:

- Letters, newsletters,
- Parents evenings
- Reference to the parents' materials on the Think U Know website (www.thinkuknow.co.uk), The UK Safer Internet Centre (www.saferinternet.org.uk) or others

Appendix 1



KS2 Computing Code of Conduct for safe and enjoyable use of our technology

- ♦ I will use school technology responsibly and carefully for school purposes only
- ♦ I will only access the school network using my own username and password
- ♦ Passwords and passcodes help protect us, I will keep mine private
- ♦ I will only open and delete my own work/files
- ♦ Where possible, I will ask before taking someone's photo and before editing or sharing their image
- ♦ I will ask permission before accessing a website, unless a member of the teaching staff has already approved that site
- ♦ I will not deliberately look for, save, or send anything that could be unpleasant or nasty
- ♦ If something upsets or worries me, or I receive messages I do not like, I will tell a member of staff immediately
- ♦ I will only open emails, messages and attachments from people I know, or my teacher has approved
- ♦ I will communicate only with people I know, or my teacher has approved
- ♦ Any messages I send, posts or comments I make, will be polite and respectful
- ♦ I know that the school may check my computer files and may monitor the websites and internet services I use
- ♦ I will be **responsible** for my behaviour when using technology because I know that these rules are to keep me **safe**
- ♦ I understand that if I deliberately break these rules, I could be stopped from using the Internet or other technologies

Computing Code of Conduct

Signed: _____

Date: _____

Appendix 2

Acceptable use policy agreement – staff & volunteer

Background

Technology has transformed learning, entertainment and communication for individuals and for all organisations that work with young people. However, the use of technology can also bring risks. All users should have an entitlement to safe internet access at all times.

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people

.

For my professional and personal safety:

- I understand that the school can monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to the use of school ICT systems (laptops, email, iPads) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school in the e-safety policy.
- I will not disclose my username or password to anyone else, nor will I try to use anyone else's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language, and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others, I will do so with their permission and in accordance with the school's policy on the use of digital images. I will not use my personal equipment to record these images unless I have permission to do so. Where these images are published, on the school website, it will not be possible to identify by name or other personal information those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- I will only use my personal mobile ICT devices as agreed in the e-safety policy and then in the same way as if I were using school equipment. I will ensure that any such devices are protected by up-to-date antivirus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems except in an emergency

- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy. Where personal data is transferred outside the secure school network, it must be encrypted.
- I understand that the data protection policy requires that any staff or pupil data to which I have access will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software; however, this may have happened.

When using the internet in my professional capacity or for sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could involve a warning, a suspension, referral to Governors and in the event of illegal activities, the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) within these guidelines.

Name:
Signed:
Date: