KEREM SCHOOL
(Including Kerem Early Years Unit)

E-Safety Policy

Kerem School believes the potential that technology has to impact on the lives of all citizens increases year on year. In many areas technology is transforming the way that schools teach and that 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
- Unauthorised access to / loss of / 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 on 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 over the technical structures we put in place to keep them safe) and so this policy also sets out how we educate children of 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 Co-ordinator
Our ICT Co-ordinator is the person responsible to the Head Teacher and Governors for the day to day issues relating to e-safety.

The ICT Co-ordinator:

- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school 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 / un blocking to the IT technicians Nippy Gecko
- Ensuring that the children are taught by the ICT teacher and other staff about e-safety.

Responsibilities: Governors
Our Governors are responsible for the approval of this policy and for reviewing its effectiveness. This will be carried out by the Governors.

Responsibilities: Head Teacher

- The Head Teacher is 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 ICT Co-ordinator
- The Head Teacher and another member of the senior management team 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 of 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 Co-ordinator
- 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.

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 ICT Co-ordinator or Head Teacher 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, 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 within this policy and associated behaviour and 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)
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)
• Parents / carers (including permissions to use pupil images / work and to use ICT systems)
• Community users of the school's ICT system

Acceptable use policies are revisited and resigned annually at the start of each school year and amended accordingly in the light of new developments and discussions with the children which take place at the 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 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 cyber bullying
- PSHE E-Safety has links to this – staying safe

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 a 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 web sites (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 generates 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 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 (eg 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
• On-line 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 hand held technology (mobile phones/ iPads/tablets 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 required to use their own professional judgement as to when it is appropriate to use them. Broadly speaking this is:
- iPads can be used in lesson times
- Members of staff are free to use these devices in school, outside teaching time in the staffroom and office.

• Y6 Pupils are currently permitted to bring their personal mobile phones into school, but these must be handed in to the school office each morning.

A number of iPads are available in school and are used by children as considered appropriate by members of staff.

Mobile phones should only be used in the office and staffroom for emergency use. There are school mobile phones that should be used on trips etc rather than personal mobile phones.

Mobile phone use in the EYU

To ensure 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 ensure 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 at 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.
- Personal mobile phones should only be used in staff rooms on both sites or in the office.
- The Early Years Co-ordinator 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 eg. 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

See also the following section for guidance on publication of photographs

Use of web-based publication tools

Our school uses the public facing website, www.kerem.org.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 pupil's 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.

The views and experiences of pupils are used to inform this process also.

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 out 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.
• Bring in outside speakers to provide added education for KS2.
• 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 in the monitoring and regulation of the children's on-line 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

Reviewed September 2017. Next Review January 2019.