King's Park Primary School



E-Safety Policy
And
Acceptable Use Agreement

Introduction

Information and Communications Technology (ICT) covers a wide range of resources including web-based and mobile learning. Currently the internet technologies children and young people are using, both inside and outside of the classroom, include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

Whilst these ICT resources can be exciting and beneficial both in and out of the context of education, all users need to be aware of the range of risks associated with the use of Internet technologies.

In King's Park Primary School we understand the responsibility to educate our pupils in e-Safety issues. We aim to teach them appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

The Internet

The Internet is a unique and exciting resource. It brings the world into the classroom by giving children access to a global network of educational resources. There is no doubt that the use of the Internet is an essential skill for children as they grow up in the modern world. The Internet is, however, an open communications' channel, available to all. Anyone can send messages, discuss ideas and publish materials with little restriction. This brings young people into contact with people from all sectors of society and with a wide variety of materials some of which could be unsuitable. Key Concerns are:

Potential Contact

Children may come into contact with someone on-line who may wish to harm them. Some adults use social networks, chat rooms or e-mail to communicate with children for inappropriate reasons

Children should be taught:

- That people are not always who they say they are.
- That "Stranger Danger" applies to the people they encounter through the Internet.
- That they should never give out personal details or
- That they should never meet alone anyone contacted via the Internet, and
- That once they publish information it can be disseminated with ease and cannot be destroyed.

Inappropriate Content

Through the Internet there are unsuitable materials in many varieties. Anyone can post material on the Internet.
Some material is published for an adult audience and is unsuitable for children e.g. materials with a sexual content.
Materials may express extreme views. E.g. some use the web to publish information on weapons, crime and racism which would be restricted elsewhere.
Materials may contain misleading and inaccurate information. E.g. some use the web to promote activities which are harmful such as anorexia or bulimia.

Children should be taught:-

- That information on the Internet is not always accurate or true.
- To question the source of information.
- How to respond to unsuitable materials or requests and that they should tell a teacher/adult immediately.

If children are to use the Internet in places other than at school e.g. – libraries, clubs and at home, they need to be educated about how to behave on-line and to discuss problems. There are no totally effective solutions to problems of Internet safety. Teachers, pupils and parents must be vigilant.

Roles and Responsibilities

As e-Safety is an important aspect of strategic leadership within the school, the Principal and Board of Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. It is the role of the ICT Co-ordinator to keep abreast of current e-safety issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet. The ICT Co-ordinator has responsibility for leading and monitoring the implementation of e-safety throughout the school.

The Principal/CT Co-ordinator update Senior Management and Governors with regard to e-safety and all governors have an understanding of the issues at our school in relation to local and national guidelines and advice.

Writing and Reviewing the e-Safety Policy

This policy, supported by the school's Acceptable Use Agreement for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to other school policies including those for ICT, Behaviour, Health and Safety, Child Protection, and Anti-bullying. The e-Safety policy and its implementation will be reviewed annually.

E-Safety Skills' Development for Staff

- All staff receive regular information and training on e-Safety issues through the co-ordinator at staff meetings.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community.
- New staff members receive information on the school's Acceptable Use Agreement as part of their induction.
- All staff are encouraged to incorporate e-Safety activities and awareness within their lessons.

E-Safety Information for Parents/Carers

- Parents/carers are asked to read through and sign the Acceptable Use Agreement on behalf of their child.
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used on the school website.
- The school website contains useful information and links to sites like CEOP's thinkuknow, Childline, and the CBBC Web Stay Safe page.
- The school will communicate relevant e-Safety information through newsletters and the school website.

Parents should remember that it is important to promote e-Safety in the home and to monitor Internet use.

- Keep the computer in a communal area of the home.
- Be aware that children have access to the internet via gaming stations and portable technologies such as smart phones.
- Monitor on-line time and be aware of excessive hours spent on the Internet.
- Take an interest in what children are doing. Discuss with the children what they are seeing and using on the Internet.
- Advise children to take care and to use the Internet in a sensible and responsible manner. Know the SMART tips.
- Discuss the fact that there are websites/social networking activities which are unsuitable.
- Discuss how children should respond to unsuitable materials or requests.
- Remind children never to give out personal information online.
- Remind children that people on line may not be who they say they are.
- Be vigilant. Ensure that children do not arrange to meet someone they meet on line.
- Be aware that children may be using the Internet in places other than in their own home or at school and that this internet use may not be filtered or supervised.

Teaching and Learning

Internet use:

- The school will plan and provide opportunities within a range of curriculum areas to teach e-Safety.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the e-Safety curriculum.
- Pupils are aware of the impact of online bullying and know how to seek help if these issues affect them. Pupils are also aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/carer, teacher/trusted member of staff, or an organisation such as Childline/CEOP.
- The school Internet access is filtered through the C2k managed service.
- No filtering service is 100% effective; therefore all children's use of the Internet is supervised by an adult.
- Use of the Internet is a planned activity. Aimless surfing is not encouraged. Children are taught to use the Internet in response to a need e.g. a question which has arisen from work in class.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Children are taught to be Internet Wise. Children are made aware of Internet Safety Rules and are encouraged to discuss how to cope if they come across inappropriate material.

E-mail:

- Pupils may only use C2k e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- The forwarding of chain mail is not permitted.
- Children are not always given individual e-mail addresses. In some instances children may have access to a group e-mail address to communicate with other children as part of a particular project. Messages sent and received in this way are supervised by the teacher.

Social Networking:

- The school C2k system will block access to social networking sites.
- Pupils and parents will be advised that the use of social networking is inappropriate for primary aged pupils. However, we accept that some pupils will still use them; they will be advised never to give out personal details of any kind, which may identify them or their location.
- Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Our pupils are asked to report any incidents of bullying to the school.
- School staff will not add children as 'friends' if they use these sites.

Mobile Technologies:

- The use of portable media such as memory sticks and external hard drives will be monitored closely as potential sources of computer virus and inappropriate material.
- Staff should not store pupils' personal data and photographs on memory sticks.
- Pupils are not allowed to use personal mobile devices/phones (in school) during class.
- Staff should not use personal mobile phones during designated teaching sessions.

Managing Video-conferencing:

- Videoconferencing will be via the C2k network to ensure quality of service and security.

Publishing Pupils' Images and Work

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website. This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue.
- Parents/carers may withdraw permission, in writing, at any time.
- Photographs that include pupils will be selected carefully and **will not** enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the School Website, particularly in association with photographs.
- Photographs of individual pupils will not be permitted. Only pictures of groups or group activities will be used.
- Pupil's work can only be published by outside agencies with the permission of the pupil and parents.

Policy Decisions:

Authorising Internet access

- Pupil instruction in responsible and safe use should precede any Internet access and all children must sign up to the Acceptable Use Agreement for pupils and abide by the school's e-Safety rules. These e-Safety rules will also be displayed clearly in all rooms.
- Access to the Internet will be supervised.
- All parents will be asked to sign the Acceptable Use Agreement for pupils giving consent for their child to use the Internet in school by following the school's e-Safety rules and within the constraints detailed in the school's e-Safety policy.
- All staff must read and agree in writing to adhere to the Acceptable Use Agreement for Staff before using any school ICT resource.

Password Security:

- Adult users are provided with an individual login username and password, which they are encouraged to change periodically. Login details should not be shared with pupils.
- All pupils are provided with an individual login username and password.
- Pupils are not allowed to deliberately access files on the school network which belong to their peers, teachers or others.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school network.

Handling e-Safety Complaints:

- Complaints of internet misuse will be dealt with by a senior member of staff.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the ICT Co-ordinator and recorded in the e-Safety incident logbook.
- Any complaint about staff misuse must be referred to the Principal.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints' procedure.

Communicating the Policy:

Introducing the e-Safety Policy to pupils

- e-Safety rules will be displayed in all classrooms and the ICT suite and discussed with the pupils at the start of each year. Specific lessons will be taught by class teachers at the beginning of every year and at relevant points throughout e.g. during PDMU lessons/circle times/anti-bullying week.
- Pupils will be informed that network and Internet use will be monitored**.**

.

Staff and the e-Safety Policy:

- All staff will be given the School e-Safety Policy and its importance explained.
- Any information downloaded must be respectful of copyright, property rights and privacy.
- Staff should be aware that Internet traffic could be monitored and traced to the individual user. Discretion and professional conduct is essential.
- A laptop issued to a member of staff remains the property of the school. Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to Internet access, data protection and use of software, both in and out of school.

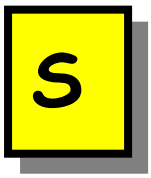
Monitoring and review:

This policy is implemented on a day-to-day basis by all school staff and is monitored by the ICT Co-ordinator.

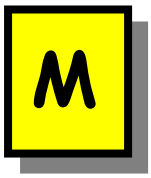
This policy is the Governors' responsibility and they will review its effectiveness annually. They will do this during reviews conducted between the ICT Co-ordinator and Designated Child Protection Co-ordinator.

Safety Rules for Children

Follow These SMART TIPS



Secret - Always keep your name, address, mobile phone number and password private – it's like giving out the keys to your home!



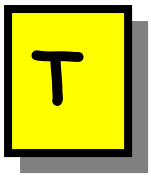
Meeting someone you have contacted in cyberspace can be dangerous. Only do so with your parent's/carer's permission, and then when they can be present.



Accepting e-mails or opening files from people you don't really know or trust can get you into trouble – they may contain viruses or nasty messages.



Remember someone on-line may be lying and not be who they say they are. Stick to the public areas in chat rooms and if you feel uncomfortable simply get out of there!



Tell your parent or carer if someone or something makes you feel uncomfortable or worried.

SMART Tips from: – Helping your parents be cool about the Internet, produced by: Northern Area Child Protection Committees

An Acceptable Use of the Internet

Children should know that they are responsible for making an Acceptable Use of the Internet. They must discuss and agree rules for this Acceptable Use. Parents are also asked to be aware of the code of Acceptable Use and confirm that their children will follow these rules.

- On the network, I will only use my own login username and password.
- I will keep my username and password private.
- I will not access other people's files without their permission.
- I will not change or delete other people's work/files.
- I will ask permission before entering any website, unless my teacher has already approved that site.
- I will use the Internet for research and school purposes only.
- I will only send e-mail which my teacher has approved. I will make sure that the messages I send are polite and responsible.
- I understand that the use of strong language, swearing or aggressive behaviour is not allowed when using e-mail etc.
- When sending e-mail I will not give my name, address or phone number or arrange to meet anyone.
- I understand that I am not allowed to enter Internet Chat Rooms while using school computers.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.
- I will not bring in memory sticks or CD Roms from home to use in school unless I have been given permission by my class teacher.
- I understand that the school may check my computer files/Emails and may monitor the Internet sites that I visit.
- I will always quote the source of any information gained from the Internet i.e. the web address, in the documents I produce.
- I understand that if I deliberately break these rules I could be stopped from using the Internet/E-mail and my parents/cares will be informed.

MOBILE PHONE POLICY

INTRODUCTION

In King's Park Primary School the welfare and wellbeing of our pupils is paramount. This policy on the use of mobile phones in school and whilst with children, has been drawn up in the best interests of pupil safety and staff professionalism.

RELATED POLICIES

Child Protection Policy
Pastoral Care Policy
Code of Conduct Policy

USE OF MOBILE PHONES

PUPILS-

- Mobile phones must be switched off when in school, and kept in the child's school bag. They are the responsibility of the child/parent, and the school will not be liable for loss or damage.

- If a child uses their phone without permission during school it will be confiscated and returned to the child at the end of the day.

- Persistent failure to follow this policy will result in the child's parents being informed and it will be requested that the phone be kept at home.

STAFF –

- Staff should have their phones on 'silent' or switched off during class time.
- Staff should not make or receive calls during teaching time. If there are extreme circumstances (eg acutely sick relative) the member of staff should make the Principal aware of this and can have their phone on in case of having to receive an emergency call.
- Use of phones must be limited to non-contact time when no children are present.

- Phones should be kept out of sight when staff are with children.

- Calls/texts must be made/received in private during non-contact time.

- Phones must never be used to take photographs of children or to store their personal data.

PARENTS AND OTHER VISITORS

- We request that parents do not use mobile phones in the school buildings or grounds.
- Mobile phones must never be used to take photographs in the school building or grounds.

We appreciate the support from all our staff in implementing this policy.

Photographic Images Policy

What does a photographic image include?
It includes video and digital photography, camera phones, CCTV, media (film and newspapers) and webcams.

Parents will be asked yearly via correspondence from school, to give their consent to have images taken of their child for media, websites, school magazine, video etc. If parents wish to change their permission they should contact the school.

If a parent does not agree to their child being photographed the staff will comply sensitively to this request.

- Schools must get consent from social workers for looked after children.
- If there is disagreement between parents/guardians it will be deemed that consent is not given.
- Consent is not required if photos and video footage are taken at public events where a significant number of individuals are captured.

What should happen when parents and a pupil disagree on consent?
1.When parental consent has been given and the pupil does not wish to be photographed the pupil's wish should be respected.
2.When a pupil wishes to appear in a photograph and the parents have not given consent then the parent's wishes should be respected.
3.When parents disagree about giving consent then schools should treat the situation as if consent had not been given.

Media and Newspapers

Team Photographs/Photo opportunities
- When photographs and names are allowed to be published, publication can occur.
- If a parent is not happy to have a child's name printed on a photograph then consideration should be given to publishing the photo with no names.

Considerations for Child Protection
Digital technology makes it easier for pictures and images to be used inappropriately as printed material on the web. Photographs can be used as a means of identifying children when they are accompanied with personal information. The content can also be used or adapted for inappropriate use.

Any concerns regarding inappropriate use of images should be reported to the Designated Teachers/Principal.

King's Park Primary and Nursery School

Staff ICT Acceptable Use Policy 2024/25

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

· I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, PDAs, digital cameras, email and social media sites**.**

· School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

· I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

· I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system).

· I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.

· I will only stream video/audio clips that I have previewed thoroughly from all sources including YouTube and take responsibility for all content shown.

· I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1988. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls) or accessed remotely. Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a

method approved by the school. Any images or videos of pupils will only be used as stated in the school image use policy and will always take into account parental consent.

· I will not keep professional documents which contain school-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are secured and encrypted. Where possible I will use the School Learning Platform 'MYFILES' to upload any work documents and files in a password protected environment in compliance with GDPR.

· I will protect the devices in my care from unapproved access or theft.

· I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.

· I will respect copyright and intellectual property rights.

· I have read and understood the school e-Safety policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.

· I will report all incidents of concern regarding children's online safety to the Designated Child Protection Coordinator Mr Kirkland and the Deputy Designated teachers Mr Mawhinney / Mrs Woods / Mrs Quinn / Mrs Thompson / Mr A Shields and/or the ICT Coordinators (Mr Shields, Mrs Stafford) as soon as possible

·I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to (Mr Shields, Mrs Stafford) the ICT Coordinators / the designated lead for filtering as soon as possible.

· I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any school related documents or files, then I will report this to the ICT Support Provider/Team (C2K) as soon as possible. ICT Co-ordinators should be informed.

· My electronic communications with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address, telephone number or ClassDojo. Any pre-existing relationships which may compromise this will be discussed with the Senior Management team.

· My use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. My use of ICT will not interfere with my work duties and will be in accordance with the school Acceptable Use Policy and the Law.

· I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the Education Authority, into disrepute.

· I will promote e-Safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

· If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the ICT Coordinators or the Principal.

· I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read, understood and agree to comply with the Staff ICT Acceptable Use Policy.

Signed: ……..... Print Name: …… Date: ……

Accepted by: …… Print Name: ……

King's Park Primary School provides Apple iPads for staff to enable them to carry out their job role more effectively. Please sign below to accept this iPad and agree to the following terms of use:

1. This iPad remains the property of King's Park Primary School and is loaned to you for use within your job role.
2. The iPad must remain in your possession, should only be used by you and should be securely stored when not in use.
3. All iPad use must fully comply with the King's Park Primary School e-Safety Policy and Data Protection Policy. Failure to do so may lead to disciplinary action.
4. The iPad may be connected to your school email account which may have access to the personal information of pupils. The iPad might also be used to store personal information such as picture and video images of pupils. This means you must fully comply with high standards of data protection.
5. This iPad has been configured with certain restrictions in place. You must not remove the designated iTunes account or sync with personal Apple devices / software. The default passcode required has been configured to 0000 should you wish to change the passcode you must inform an ICT Co-Ordinator with new passcode.
6. Loss or damage of the device should be reported to the *Headteacher / ICT Co-ordinator* immediately. If necessary the device will be remotely locked or wiped.
7. Insurance cover provides protection from the standard risks whilst the iPad is on the school site **but excludes** theft from your car or from other establishments. Should you damage, or leave the iPad unattended and it is stolen, you will be responsible for its replacement and may need to claim this from your own insurance company.
8. The iPad will be used in the classroom for teaching and learning. Remember that personal information might be accessible on the device and you must fully comply with high standards of data protection, therefore supervision of pupil use is required.
9. All app purchases of a chargeable value must be cleared by an ICT co-ordinator.
10. This iPad will be checked annually for safety and for compliance with school policies. Outcomes will be reported to the Headteacher.
11. If you leave the employment of the school the iPad must be returned in good condition to the *Headteacher / Co-ordinator* before your official leaving date.

iPad number: .....

Authorised by Co-ordinator: ..... Date: .....

Member of Staff: .....

I have read this agreement and fully understand that I need to adhere to all elements.

Received by Signature: ..... Date: .....