KING'S OAK PRIMARY SCHOOL

Online Safety
and
Data Security Policy
September 2020

Policy prepared/reviewed by: Catherine Giles

Policy reviewed and approved by: Governing Body

Date of approval: 24.09.2020

Date of next review: September 2022

Acknowledgements:

Hertfordshire County Council

Introduction

ICT is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to develop in our children the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. The internet technologies children and young people use both inside and outside of the classroom include:

- Websites
- E-mail, Instant Messaging and chat rooms
- Social Media e.g. Facebook, Twitter, Instagram, Tik Tok, WhatsApp etc.
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality
- Gaming, especially online
- Virtual Learning Environments e.g. Google Classroom
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies and that some have minimum age requirements, usually 13 years.

At King's Oak Primary School, we understand the responsibility to educate our pupils on online safety issues, teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can also result in media coverage, and potentially damage the reputation of the school.

Everybody in the school has a shared responsibility to adhere to the Data Protection Policy and secure any personal or sensitive information used in their day to day professional duties and ALL staff are aware of the risks and threats and how to minimise them. Failure to follow the Data Protection Policy may result in action being taken under the Disciplinary Procedure.

Both this policy and the Acceptable Use Agreement for all staff (throughout this policy 'staff' includes governors, visitors and other adults in school) and pupils are inclusive of both fixed and mobile internet technologies provided by the school (such as PCs, laptops, Chromebooks, mobile devices, webcams, whiteboards, digital video equipment, etc.) and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

Monitoring

All electronic activity is logged by the school's internet provider and locally installed software – Securus - which takes screen shots of all use which could raise safeguarding concerns. These logs are monitored daily by authorised staff.

Authorised staff may also, under direction of the Headteacher and without prior notice, access the e-mail and voice-mail accounts and the private network drive of someone who is absent (and whom it has not been possible to contact) in order to deal with any business-related issues retained on that account.

Breaches

A breach or suspected breach of policy by a school employee, visitor, volunteer or pupil may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the alleged offending individual.

Any policy breach by staff is grounds for disciplinary action in accordance with the school Disciplinary Procedure. Policy breaches may also lead to criminal or civil proceedings.

Incident reporting

Any security breaches or attempts, loss or theft of equipment or data (including logons and passwords) and any unauthorised use or suspected misuse of ICT must be immediately reported to the Data Protection Officer. Additionally, all virus notifications, unsolicited emails and all other policy non-compliance must be reported to the Data Protection Officer. A log is kept of all incidents.

Acceptable Use Agreement

Pupils, staff, governors and regular visitors are required to sign the Acceptable Use Policy agreement and parents/carers are required to give their permission for children to use the internet.

Computer viruses

- All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick must be checked for any viruses using school provided anti-virus software before being used.
- Staff must never interfere with any anti-virus software installed on school ICT equipment that they use.
- If computers are not routinely connected to the school network, staff must make provision for regular virus updates through the IT team.
- If staff suspect there may be a virus on any school ICT equipment, they should stop using the equipment and notify the Data Protection Officer and Site Manager who will notify the

ICT support provider. The ICT support provider will advise staff on what actions to take and be responsible for advising others that need to know.

Data security

The accessing and appropriate use of school data is something that the school takes very seriously.

- The school gives relevant staff access to its Management Information System, with a unique username and password.
- It is the responsibility of all staff to change their passwords annually, when requested, and keep their passwords secure.
- Staff are aware of their responsibility when accessing school data.
- Staff are issued with relevant guidance documents and sign the Acceptable Use Policy agreement.
- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data.
- It is the responsibility of individual staff to ensure the security of any portable or mobile ICT equipment.
- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed.
- Anyone expecting a confidential or sensitive fax should ask the sender to notify them before it is sent.

Disposal of redundant ICT equipment

- All redundant ICT equipment will be disposed of through an authorised agency who will issue a certificate of destruction.
- Disposal of any ICT equipment will conform to current regulations.
- The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal.
- The school's disposal record will include:
    - Date on which the item was disposed.
    - Authorisation for disposal, including:
        - verification of software licensing.
        - any personal data likely to be held on the storage media.
    - How it was disposed of e.g. waste, gift, sale.
    - Name of person and / or organisation who received the disposed item.

Email

The use of e-mail is an essential means of communication for both staff and pupils. In the context of school, e-mail should not be considered private.

Managing email

- The school gives all staff their own e-mail account to use for all school business as a work based tool. This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoid the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure and change this annually, when requested. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The personal school email account should be the account that is used for all school business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses.
- All e-mails should be written and checked carefully before sending, particularly if auto-complete email addresses are used.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- E-mails created or received as part of a school role will be subject to disclosure in response to either a request for information under the Freedom of Information Act 2000 or a subject access request under the Data Protection Act 2018. Staff must therefore actively manage their e-mail account as follows:
  - Delete all e-mails of short-term value
  - Organise e-mail into folders and carry out frequent house-keeping on all folders and archives
- The forwarding of chain letters is not permitted in school. However pupils should forward any chain letters causing them anxiety after notifying their teacher.
- All pupil e-mail users are expected to adhere to the generally accepted rules of internet access, particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.
- Staff must inform the Headteacher if they receive an offensive e-mail.
- All school e-mail policies apply whenever and wherever staff access their school email account.

Sending emails

- If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, staff should ensure these are encrypted or password protected unless they are being sent to organisations with secure email addresses, as notified to staff.
- Staff should use their own school e-mail account so that they are clearly identified as the originator of a message. Staff are encouraged to send emails to parents via the admin box or other shared email boxes set up for this purpose.
- Staff should keep the number of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate.

- School e-mail is not to be used for personal advertising.

Receiving emails

Staff should:

- Check their e-mail account daily.
- Activate 'out-of-office' notification when away for extended periods.
- Never open attachments from an untrusted source; staff should consult the Data Protection Officer first.
- Not use the e-mail systems to store attachments; these should be detached and saved to the appropriate shared drive/folder.

The automatic forwarding and deletion of e-mails is not allowed.

Emailing personal, sensitive, confidential or classified information

Staff should:

- Obtain express consent from their manager to provide the information by e-mail.
- Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:
    - Encrypt and/or password protect
    - Verify the details, including accurate e-mail address, of any intended recipient of the information
    - Verify (by phoning) the details of a requestor before responding to e-mail requests for information
    - Do not copy or forward the e-mail to any more recipients than is absolutely necessary
    - Send the information as an encrypted document **attached** to an e-mail
    - Provide the encryption key or password by a **separate** contact with the recipient(s)
    - Do not identify such information in the subject line of any e-mail
    - Request confirmation of safe receipt

RBK makes provision for secure data transfers via USO.

Equal opportunities

The school endeavours to create a consistent message for all pupils and this in turn should aid establishment and future development of the school's online safety rules.

However, we are aware that some pupils may require additional support or teaching, including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of online safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of online safety. Internet activities are planned and well managed for these children.

Online Safety - roles and responsibilities

The Headteacher and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

- The named Data Protection Officer in this school is Catherine Giles. All members of the school community have been made aware of who holds this post. It is the role of the Data Protection Officer to keep abreast of current issues and guidance relating to data protection.

- New staff receive information on the school's acceptable use policy as part of their induction.
- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety and know what to do in the event of misuse of technology by any member of the school community.
- All staff are encouraged to incorporate online safety activities and awareness within their curriculum areas.

Online Safety in the curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for online safety guidance to be given to the pupils on a regular and meaningful basis. Online safety is embedded within our curriculum and we continually look for new opportunities to promote online safety.

- The Online Safety Policy will be introduced to the pupils at the start of each school year.
- The school has a framework for teaching internet skills in computing lessons.
- The school provides opportunities within a range of curriculum areas to teach about online safety.
- Educating pupils about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the computing curriculum.
- Pupils are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modelling and appropriate activities.
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by any form of online bullying. 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 staff member, or an organisation such as Childline or CEOP report abuse button.
- Pupils are taught to critically evaluate materials and learn good searching skills through discussions and via the computing curriculum.

Managing the internet

- The school provides pupils with supervised access to internet resources (where reasonable) through the school's fixed and wireless internet connectivity.
- Staff will preview any recommended sites before use.

- Image searches are discouraged when working with pupils.
- If internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. We advise parents/carers to recheck these sites and supervise this work. Parents/carers will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

Internet use

- Staff should not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience.
- Staff should not reveal names of colleagues, pupils, others or any other confidential information acquired through their job on any social networking site or other online application.
- All pupils are advised to be cautious about the information given by others on social networking sites, for example users not being who they say they are.
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on social networking sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Pupils are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests).
- Our pupils are asked to report any incidents of online bullying to school.
- Staff may only create blogs, wikis or other online areas in order to communicate with pupils using systems approved by the Headteacher.
- Staff should not access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libellous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school or RBK into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the school's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability.

It is at the Headteacher's discretion as to what internet activities are permissible for staff and pupils.

Infrastructure

- School internet access is controlled through the school's web filtering service.
- All websites will be checked by the Data Protection Officer before being unblocked and only unblocked with the permission of the Headteacher. An email containing a link to the website should be sent to the Data Protection Officer for checking.
- Only websites with proven legitimate school use will be unblocked.

- Staff will be responsible for thoroughly checking the content of websites/clips/links they wish to use for lessons, prior to their use, and only those areas previously accessed and checked may be used at school.
- To maintain safeguarding requirements, sites will not be unblocked for children's direct use unless they are from reputable providers (e.g. BBC) and their content proven to be suitable.
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
- If staff or pupils discover unsuitable sites with inappropriate content (containing only adults) the URL (address) and content should be recorded and notified to the Data Protection Officer so that the site can be blocked. If staff or pupils discover unsuitable site with illegal content (containing adults and children) the computer should have the electricity disconnected while connected to the site, after the URL (address) and content have been recorded, and secured. The Headteacher and Data Protection Officer should be informed immediately and given the details. The Headteacher will inform the police who will take the appropriate action.
- It is the responsibility of the school, by delegation to IT Support Provider, to ensure that anti-virus protection is installed and kept up-to-date on all school machines.
- If pupils wish to bring in work on removable media it must be given to the class teacher for a safety check first.

Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the class teacher (pupils) or Headteacher (staff).

Parent/carer engagement

We believe that it is essential for parents/carers to be fully involved and engaged in promoting online safety both in and outside of school and to be aware of their responsibilities. We consult and discuss online safety with parents/ carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks.

- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the school.
- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g. on school website or on school social media).

Password security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords private and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

- Staff and governors are required to change their passwords annually, when prompted.
- All users read and sign an Acceptable Use Policy agreement to demonstrate that they have understood the school's Online Safety and Data Security Policy.
- Users are provided with an individual network login and Management Information System

(where appropriate) log-in username.

- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of the school networks, MIS systems and/or learning platform, including ensuring that passwords are not shared and are changed annually. Individual staff users must also make sure that workstations are not left unattended and are locked every time they leave.

If staff believe that their password may have been compromised or someone else has become aware of their password, they should report this to the Data Protection Officer.

Protecting Personal, Sensitive, Confidential and Classified Information

Staff should:

- Ensure that any school information accessed from their own PC is kept secure.
- Ensure they lock their screen before moving away from their computer to prevent unauthorised access.
- Ensure the accuracy of any personal, sensitive, confidential and classified information they disclose or share with others.
- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person.
- Ensure the security of any personal, sensitive, confidential and classified information contained in documents they fax, copy, scan or print.
- Only download personal data from systems if expressly authorised to do so by their manager.
- Not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience.
- Keep their screen display out of direct view of any third parties when accessing personal, sensitive, confidential or classified information.
- Ensure hard copies of data are securely stored and disposed of after use in accordance with the record retention schedule.

Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media

This is not permitted unless staff have explicit permission from the Headteacher; staff have remote access to the network and are aware that work should only be saved on the network.

Remote access

- Staff are responsible for all activity via their remote access facility.
- Staff should only use equipment with an appropriate level of security for remote access.
- To prevent unauthorised access to school systems, staff should keep all access information

such as logon IDs confidential and not disclose them to anyone.

- Staff should select passwords to ensure that they are not easily guessed, e.g. not use house or telephone numbers or choose consecutive or repeated numbers.
- Staff should avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is.
- Staff should protect school information and data at all times, including any printed material produced while using the remote access facility and take particular care when access is from a non-school environment.

Safe use of images

- With the written consent of parents (on behalf of pupils), the school permits the appropriate taking of images by staff and pupils with school equipment.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils; this includes during field trips. However with the express permission of the Headteacher, images can be taken during field trips provided they are transferred immediately and solely to the school's network on return to school and deleted from the staff device.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of pupils, staff and others without advance permission from the Headteacher.
- Pupils and staff must have permission from the Headteacher before any image can be uploaded for publication.

Publishing Pupil's Images and Work

On a child's entry to our school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site or on social media.
- in the school prospectus and other printed publications that the school may produce for promotional purposes.
- recorded/ transmitted on a video or webcam.
- in display material that may be used in the school's communal areas.
- in display material that may be used in external areas, i.e. exhibition promoting the school.
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically).

This consent form is considered valid for the entire period that the child attends our school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc. Parents or carers may withdraw permission, in writing, at any time.

Pupils' names will not be published alongside their images and vice versa, except with prior permission of the parents/carers e.g. when used for the press. E-mail and postal addresses of pupils will not be published. Before posting student work on the internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Storage of Images

- Images/ films of children are stored on the school's network
- Staff are not permitted to use personal portable media for storage of images (e.g. USB sticks)–without the express permission of the Headteacher.
- Rights of access to this material are restricted to the staff and pupils within the confines of the school network or other online school resource.
- Staff are responsible for deleting the images they have taken when they are no longer required, or when the pupil has left the school.

Webcams and CCTV

The school uses CCTV for security and safety. The only people with access to this are the Headteacher, Data Protection Officer and Site Manager/Deputy Site Manager. Notification of CCTV use is displayed at all entrances to the school and in main reception.

Publicly accessible webcams are not used in school.

Video Conferencing

- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside the school.
- All pupils are supervised by a member of staff when video conferencing.
- We keep a record of video conferences, including date, time and participants.
- Approval from the Headteacher is sought prior to all video conferences within school.
- No part of any video conference is recorded in any medium without the written consent of those taking part.

Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use as long as these remain switched off during the teaching day and are only used in the staff areas. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device.
- Pupils are allowed to bring personal mobile devices/phones to school but must switch them off and hand them into the office on arrival at school.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any member of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community e.g. during concerts/assemblies etc.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device and that the device has up to date anti-virus software installed.

School Provided Mobile Devices (including phones)

- The sending of inappropriate text messages between any member of the school community is not allowed.
- Where the school provides mobile technologies such as phones, laptops, Chromebooks and iPads for offsite visits and trips, only these devices should be used.
- Where the school provides a laptop/Chromebook/iPad for staff, this device may only be used to conduct school business and only by school staff.

Servers

- Servers are kept in a locked, temperature-controlled and secure environment.
- Access rights are limited.
- Data is backed up regularly to a remote server.

Social Media, including Facebook and Twitter

Facebook, Twitter and other forms of social media are increasingly becoming an important part of our daily lives.

- Staff are not permitted to access their personal social media accounts using school equipment at any time.
- Staff are able to setup social media accounts, using their school email address, in order to be able to teach pupils the safe and responsible use of Facebook or other applications, with the prior permission of the Headteacher.
- Pupils are not permitted to access their social media accounts whilst at school.
- Staff, governors, pupils, parents and carers are aware that their online behaviour should at all times be compatible with UK law and comply with the Confidentiality Policy.

School Mobile phones

- Staff are responsible for the security of their school mobile phone.
- Staff should report the loss or theft of any school mobile phone equipment immediately.
- School SIM cards must only be used in school provided mobile phones.
- All school mobile phones are barred from calling premium rate numbers and any numbers outside of the UK as the default.
- Staff must not send text messages to premium rate services.

Review Procedure

This policy will be reviewed every two years and consideration given to the implications for future whole school development planning.