

ONLINE & E-SAFETY POLICY

This policy should be read in conjunction with the following policies and guidance:

- Safeguarding and Child Protection
- Data Protection
- Keeping Children Safe in Education 2023
- Guidance For Safer Working Practice For Those Working With Children and Young People in Education Settings 2022

INTRODUCTION

The King of Kings School understands the responsibility to educate our pupils on online safety issues (e-safety); 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.

Online safety is a key part of safeguarding so that young people do not see the internet as a separate part of their lives. The school will ensure that online safety is delivered as part of the curriculum on a regular basis.

We understand that the breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk according to KCSIE 2023:

- **content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **conduct:** online behaviour that increases the likelihood of, or causes, harm; for example, making, sending, and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and
- **commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams. If we feel any of our pupils, students or staff are at risk, it will be reported to the Anti-Phishing Working Group.

Internet, mobile and digital technologies in the 21st Century are essential resources 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 arm our young people with the skills to access life-long learning and employment.

Internet, mobile and digital technologies cover a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of internet, mobile and digital technologies within our society as a whole. Currently

the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Apps
- E-mail, Instant Messaging, and chat rooms
- Social Media, including Facebook and Twitter
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices including tablets and gaming devices
- Online Games
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video sharing
- Downloading
- On demand TV and video, movies, and radio / Smart TVs

Whilst exciting and beneficial both in and out of the context of education, much internet, mobile and digital technologies, 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 technologies and that some have minimum age requirements (13 years in most cases).

The School holds personal data on learners, staff, and others to help conduct 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 result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for the school to use technology to benefit learners.

Everybody in the school community has a shared responsibility to secure any sensitive information used in their day-to-day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreements (for all staff, Governors regular visitors [for regulated activities] and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, 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).

‘Staff’ applies to all Supervisors/Teachers/Volunteers/Governors of the school.

DATA PROTECTION

This school holds a separate Data Protection Policy, including UK GDPR.

FILTERING AND MONITORING SYSTEM

Appropriate filtering and monitoring technology on school devices and school networks form part of our online safety. We ensure we have effective monitoring strategies in place that meet our safeguarding needs

Our school's filtering and monitoring technology is the responsibility of Dr Oyebande, who is the school's Network Manager.

IT use is monitored using a filtering and monitoring system: New system January 2024

Filtering and monitoring provision will be reviewed at least annually.

The school will block harmful and inappropriate content without unreasonably impacting teaching and learning.

Our Safeguarding Governor reviews the standards and discusses with IT staff and service providers what more needs to be done to support the school in meeting this standard.

Authorised ICT staff may inspect any ICT equipment owned or leased by the school at any time without prior notice.

Authorised ICT staff may monitor, intercept, access, inspect, record, and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice, video, or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards, and procedures; to ensure the effective operation of school ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 2018, or to prevent or detect crime.

Authorised ICT staff may, without prior notice, access the e-mail or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 2018, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Please note that personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

BREACHES

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

For staff any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure or, for Support Staff, in their Probationary Period as stated.

Policy breaches may also lead to criminal or civil proceedings.

The Information Commissioner's powers to issue monetary penalties came into force on 6 April 2010, allowing the Information Commissioner's office to serve notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act.

The data protection powers of the Information Commissioner's Office are to:

- Conduct assessments to check organisations are complying with the Act;
- Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;
- Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- Prosecute those who commit criminal offences under the Act;
- Conduct audits to assess whether organisations' processing of personal data follows good practice,
- Report to Parliament on data protection issues of concern

For pupils, reference will be made to the school's Behaviour Policy.

INCIDENT REPORTING

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of internet, mobile and digital technologies must be immediately reported to the school's relevant responsible person. Additionally, all security breaches, lost/stolen equipment, or data (including remote access ID and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the relevant responsible person. The relevant responsible individuals in the school are as follows: Dr Oyebande; deputy, Mrs Justine Golamhossen

Please refer to the relevant section on Incident Reporting, e-Safety Incident Log & Infringements.

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.
- Never interfere with any anti-virus software installed on school ICT equipment.
- If a machine is not routinely connected to the school network, provision must be made for regular virus updates through the IT team.
- If a virus is suspected on any school ICT equipment, the use of the equipment must be stopped and the ICT support provider contacted immediately. The ICT support provider will advise 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.

Security of Confidential / Personal Data - Electronic and Paper

It is critical that the school considers the safety of confidential / personal data removed from a school site (electronic and paper).

All staff are made aware of how to handle sensitive or personal information.

SECURITY

- The school gives relevant staff access to its Management Information System, with a unique username and password.
- It is the responsibility of everyone to keep passwords secure.
- Staff are aware of their responsibility when accessing school data.
- Staff have been issued with the relevant guidance documents and the ICT Acceptable Use Agreement.
- Staff keep all school related data secure. This includes all personal, sensitive, confidential, or classified data
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight
- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under control at all times
- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential, and classified information contained in documents copied, scanned, or printed. This is particularly important when shared copiers (multi-function print, scan, and copiers) are used

PROTECTIVE MARKING OF OFFICIAL INFORMATION

Staff must be trained to understand that they are personally responsible for securely handling any information that is entrusted to them, in line with local business processes.

- There is no requirement to mark routine OFFICIAL information.
- Optional descriptors can be used to distinguish specific type of information.
- Use of descriptors is at an organisation's discretion.
- Existing information does not need to be remarked.

In such cases where there is a clear and justifiable requirement to reinforce the 'need to know', assets should be conspicuously marked: '**OFFICIAL-SENSITIVE**'

RELEVANT RESPONSIBLE PERSONS

Senior members of staff should be familiar with information risks and the school's response.

The Senior Information Risk Owner (SIRO) in this school is Dr Dele Oyebands, the Safeguarding Governor who has the following responsibilities:

- they lead on the information risk policy and risk assessment.
- they advise school staff on appropriate use of school technology.
- they act as an advocate for information risk management.

The Office of Public Sector Information has produced [Managing Information Risk](http://www.nationalarchives.gov.uk/services/publications/information-risk.pdf), [\[http://www.nationalarchives.gov.uk/services/publications/information-risk.pdf\]](http://www.nationalarchives.gov.uk/services/publications/information-risk.pdf) to support relevant responsible staff members in their role.

INFORMATION ASSET OWNER (IAO)

Any information that is sensitive needs to be protected. This will include the personal data of learners and staff; such as assessment records, medical information, and special educational needs data. A responsible member of staff should be able to identify across the school:

- what information is held, and for what purposes;
- what information needs to be protected, how information will be amended or added to over time;
- who has access to the data and why; and
- how information is retained and disposed of.

As a result, this manager can manage and address risks to the information and make sure that information handling complies with legal requirements. In a Secondary School, there may be several individuals, whose roles involve such responsibility.

However, it should be clear to all staff that the handling of secured data is everyone's responsibility – whether they are an employee, consultant, software provider or managed service provider. Failing to apply appropriate controls to secure data could amount to gross misconduct or even legal action.

The IAO in this school is Justine Golamhossen

DISPOSAL OF REDUNDANT ICT EQUIPMENT POLICY

- All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data
- All redundant ICT equipment that may have held personal data will have the storage media overwritten multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen
- Disposal of any ICT equipment will conform to:

The Waste Electrical and Electronic Equipment Regulations 2006

The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007

<http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx>

http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf

http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=e

Data Protection Act 2018

[ico education-data](#)

Electricity at Work Regulations 1989

http://www.opsi.gov.uk/si/si1989/Uksi_19890635_en_1.htm

- 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 item disposed of
 - 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 & / or organisation who received the disposed item

* If personal data is likely to be held the storage media will be over written multiple times to ensure the data is irretrievably destroyed.

- Any redundant ICT equipment being considered for sale / gift will have been subject to a recent electrical safety check and hold a valid PAT certificate

Further information available at:

Waste Electrical and Electronic Equipment (WEEE) Regulations

Environment Agency web site

Introduction

<http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx>

The Waste Electrical and Electronic Equipment Regulations 2006

http://www.opsi.gov.uk/si/si2006/ukxi_20063289_en.pdf

The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007

http://www.opsi.gov.uk/si/si2007/pdf/ukxi_20073454_en.pdf?lang= e

Information Commissioner Website

<https://ico.org.uk/>

Data Protection Act – data protection guide

<https://ico.org.uk/for-organisations/education/>

ONLINE/VIRTUAL TEACHING

If the school needs to use online or virtual teaching the school will:

- ensure all relevant staff are briefed so they understand the policies and the standards of conduct expected of them.
- set clearly defined operating times for virtual learning.
- consider the impact that virtual teaching may have on children and their parents/ carers / siblings.
- determine whether there are alternatives to virtual teaching in 'real-time' - e.g., using audio only, pre-recorded lessons, existing online resources.
- ensure senior staff and DSL are able to drop in to any virtual lesson at any time – the online version of entering a classroom; therefore the school will make these people

aware of the virtual learning timetable and ensure they have the capacity to join a range of lessons

- take into account any advice published by the local authority, or their online safety / monitoring software provider.

Whilst using online or virtual teaching staff should:

- adhere to their establishment's policy on using online or virtual teaching as laid out here.
- be appropriately dressed.
- think about the background; photos, artwork, identifying features, mirrors - ideally the backing should be nondescript.
- ensure staff and pupils are in living / communal areas - no bedrooms.
- ensure all resources / videos are age appropriate.
- ensure that the Headteacher is aware that the online lesson / meeting is taking place and for what purpose.
- avoid one-to-one situations - request that a parent is present in the room for the duration or ask a colleague or member of the SLT to join the session.
- only record lessons or online meetings with a pupil where this has been agreed with the Headteacher or Deputy Head, and the pupil and their parent / carer have given explicit written consent to do so.
- be able to justify images of pupils in their possession.

This means that adults should **not**:

- contact pupils outside the operating times defined by the Headteacher
- take or record images of pupils for their personal use
- record virtual lessons or meetings using personal equipment (unless agreed and risk assessed by senior staff).
- engage online while children are in a state of undress or semi-undress.

It is the responsibility of the staff member to act as a moderator; raise any issues of suitability (of dress, setting, behaviour) with the child and / or parent immediately and end the online interaction if necessary.

Recording lessons does not prevent abuse. If staff wish to record the lesson they are teaching, consideration should be given to data protection issues; e.g., whether parental / pupil consent is needed and retention / storage.

If a staff member believes that a child or parent is recording the interaction, the lesson should be brought to an end or that child should be logged out immediately.

Staff, parents and pupils should be aware of the standards of conduct required.

If staff need to contact a pupil or parent by phone and do not have access to a work phone, they should discuss this with the Headteacher and, if there is no alternative, always use 'caller withheld' to ensure the pupil / parent is not able to identify the staff member's personal contact details.

EMAIL

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

mail can offer significant benefits including direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an e-mail in relation to their age and how to behave responsible online.

MANAGING E-MAIL

- 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 avoids the risk of personal profile information being revealed
- Staff should use their school email for all professional communication.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged, if necessary, e-mail histories can be traced. The 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
- The school requires a standard disclaimer to be attached to all e-mail correspondence, stating that, 'the views expressed are not necessarily those of the school'. The responsibility for adding this disclaimer lies with the account holder
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper
- Staff sending e-mails to external organisations, parents or children/students should copy in the Headteacher
- 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 the school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. Therefore e-mail accounts must be actively managed as follows:
 - All e-mails of short-term value must be deleted.
 - E-mails must be organised into folders and frequent housekeeping carried out on all folders and archives
- The following pupils have their own individual school issued accounts:
 - all other children use a class/ group e-mail address
- The forwarding of chain emails is not permitted in school. The school may set up a dummy account for students to forward chain emails to. No action will be taken on this account.
- All student e-mail users are expected to adhere to the generally accepted rules of responsible online behaviour 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, virus checking attachments

- Students must immediately tell a teacher/ trusted adult if they receive an offensive or upsetting e-mail.
- Staff must inform (the e-Safety coordinator or Headteacher if they receive an offensive e-mail.
- Students are introduced to e-mail as part of the ICT Programme of Study.
- In whatever way school e-mails are accessed (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply.

SENDING E-MAILS

- If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section *E-Mailing Personal, Sensitive, Confidential or Classified Information*.
- The school e-mail account should be used so that the originator of a message is clearly identified.
- The number and relevance of e-mail recipients must be kept, particularly those being copied, to the minimum necessary and appropriate.
- School e-mail is not to be used for personal advertising.

RECEIVING E-MAILS

- E-mails should be checked regularly.
- An 'out-of-office' notification should be activated when away for extended periods.
- Attachments from an untrusted source should never be opened; the network manager should be contacted first.
- E-mail systems should not be used to store attachments. Business related work should be detached and saved to the appropriate shared drive/folder.
- The automatic forwarding and deletion of e-mails is not allowed.

E-MAILING PERSONAL, SENSITIVE, CONFIDENTIAL OR CLASSIFIED INFORMATION

Where the conclusion is that e-mail must be used to transmit such data, express consent must be obtained from Headteacher or Deputy Head to provide the information by e-mail. Caution should be exercised when sending the e-mail and these checks always followed before releasing the e-mail:

- Encrypt and 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.
- Do not send the information to any person whose details have not been separately verified (usually by phone).
- 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.

EQUAL OPPORTUNITIES: PUPILS WITH ADDITIONAL NEEDS

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' e-Safety rules.

However, staff should be aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-Safety issues.

Where a pupil has poor social understanding, careful consideration should be given to group interactions when raising awareness of e-Safety. Internet activities should be planned and well managed for these children and young people.

E-SAFETY ROLES AND RESPONSIBILITIES

As e-Safety is an important aspect of strategic leadership within the school, the Headteacher and the Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

The named e-Safety Safeguarding Officer in this school is Dr Dele Oyebande, who has been designated this role as a member of the senior leadership team. All members of the school community have been made aware of who holds this post.

It is the role of the e-Safety Safeguarding Officer to keep abreast of current issues and guidance through organisations such as the LEA, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management and Governors are updated by the e-Safety Safeguarding Officer and all Governors understand the issues and strategies at our school in relation to local and national guidelines and advice.

This policy, supported by the school's Acceptable Use Agreements for staff, Governors, visitors, and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home-school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PSHE.

E-SAFETY IN THE CURRICULUM

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

The school teaches internet skills via the Khan Academy programme used with students in ICT 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 e-Safety curriculum.
- Students are to be made aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.

- Pupils are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modeling, and appropriate activities.
- Pupils are aware of the impact of Cyberbullying 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 Cybermentors, Childline or CEOP report abuse button.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the Computing curriculum.

E-SAFETY SKILLS DEVELOPMENT FOR STAFF

- Our staff receive regular information and training on e-Safety and how they can promote the 'Stay Safe' online messages in Staff Meetings, where Safeguarding is an item on the weekly agenda.
- New staff receive information on the school's Acceptable Use Agreements as part of their induction.
- All staff are to be made aware of their 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 (see e-Safety Coordinator).
- Staff are encouraged to incorporate e-Safety activities and awareness within their curriculum areas and ensure they are adequately informed with up-to-date areas of concern.

MANAGING THE SCHOOL ONLINE E-SAFETY MESSAGES

- We endeavour to embed Online e-Safety messages across the curriculum whenever the internet and/or related technologies are used.
- The Online e-Safety Policy will be introduced to students at the start of each school year.
- The key online e-Safety advice will be promoted widely throughout school

INCIDENT REPORTING, ONLINE E-SAFETY & INFRINGEMENTS

INCIDENT REPORTING

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's relevant responsible person or e-Safety Coordinator. Additionally, all security breaches, lost/stolen equipment, or data (including remote access ID and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the Information Asset Owner.

E-SAFETY INCIDENT LOG

Some incidents may need to be recorded if they relate to a bullying, extremism, or racist incident.

MISUSE AND INFRINGEMENTS

COMPLAINTS

Complaints and/ or issues relating to e-Safety should be made to the e-Safety Safeguarding Officer or Headteacher.

All incidents should be logged.

INAPPROPRIATE MATERIAL

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the e-Safety Safeguarding Officer
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the relevant responsible person, and an investigation by the Headteacher. Depending on the seriousness of the offence, sanctions could include immediate suspension, possibly leading to dismissal and involvement of police for very serious offences
- All users are to be made aware of sanctions relating to the misuse or misconduct.

See the Manchester LA Flowchart for Managing an e-Safety Incident

(Safeguarding and Child Protection Policy)

INTERNET ACCESS

The internet is an open worldwide communication medium, available to everyone, at all times. Anyone can view information, send messages, discuss ideas, and publish material which makes it both an invaluable resource for education, business, and social interaction, as well as a potential risk to young and vulnerable people.

MANAGING THE INTERNET

- The school provides pupils with supervised access to Internet resources through the school's fixed and mobile internet connectivity, except in small group ICT Lessons where the students bring their own device, connected to the internet through a single line and supervised by the teacher.
- Staff will preview any recommended sites, online services, software, and apps before use.
- Searching for images through open search engines is 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. It is advised that parents recheck these sites and supervise this work. Parents 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

- Personal, sensitive, confidential, or classified information must not be posted or such information disseminated in any way that may compromise the intended restricted audience.
- Names of colleagues, pupils, others, or any other confidential information acquired through the working at the school must not be revealed on any social networking site or other online application.
- On-line gambling or gaming is not allowed in school or on school devices.

It is at the s discretion as to what internet activities are permissible for staff and pupils and how this is disseminated.

INFRASTRUCTURE

- This school is aware of its responsibility when monitoring staff communication under current legislation and considers; Data Protection Act 2018, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.
- Staff and students are aware that school-based email and internet activity can be monitored and explored further if required.
- The school does not allow pupils access to internet logs.
- The school uses management control tools for controlling and monitoring workstations
- If staff or students discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety coordinator or teacher as appropriate.
- It is the responsibility of the school, by delegation to the network manager, to ensure that anti-virus protection is installed and kept up to date on all school machines.
- Students and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is neither the school's responsibility nor the network managers to install or maintain virus protection on personal systems. If students wish to bring in work on removable media, it may be required to be given a safety check first.
- Students and staff are not permitted to download programs or files on school-based technologies without seeking prior permission from the Headteacher, the Network manager or the ICT Lead.
- If there are any issues related to viruses or anti-virus software, the network manager should be informed via the Headteacher or the Deputy Head.

MANAGING OTHER ONLINE TECHNOLOGIES

Online technologies (including social networking sites, if used responsibly both outside and within an educational context) can provide easy to use, creative, collaborative, and free facilities. However, it is important to recognise that there are issues regarding the

appropriateness of some content, contact, culture, and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- The school endeavours to deny access to social networking and online games websites to students within school.
- All students are told to be cautious about the information given by others on such websites, for example users not being who they say they are.
- Students are taught to avoid placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Students are 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 students are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals.
- Students are encouraged to be wary about publishing specific and detailed private thoughts and information online.
- Students are asked to report any incidents of Cyberbullying to the school.
- Staff may only create blogs, wikis, or other online areas in order to communicate with pupils using the school learning platform or other systems approved by the Head teacher.
- Services such as Facebook and Instagram have a 13+ age rating which should not be ignored <http://www.coppa.org/comply.htm>

PARENTAL INVOLVEMENT

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

- Parents/carers and students are encouraged to contribute to adjustments or reviews of the school Online e-Safety Policy by (*state how*).
- 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 decide as to whether they consent to images of their child being taken and used in the public domain (e.g. on the school website).
- Parents/carers are expected to sign an Acceptable Use Agreement.
- The school disseminates information to parents relating to e-Safety where appropriate
 - Information evenings

PASSWORDS AND PASSWORD SECURITY

PASSWORDS

- Personal passwords must always be used by staff members.
- Personal passwords must be entered each time staff logon. Passwords must not be included in any automated logon procedures.
- Staff should change temporary passwords at first logon.
- Passwords must be changed whenever there is any indication of possible system or password compromise.
- Passwords or encryption keys must not be recorded on paper or in an unprotected file.
- **Personal passwords should only be disclosed to authorised ICT support staff when necessary, and never to anyone else.** All personal passwords that have been disclosed must be changed once the requirement is finished.
- **Staff should never tell a child or colleague their password.**
- **Dr Oyebands or the Headteacher must be informed immediately if there is a breach of security with password or account information.**
- User ID and passwords for staff and pupils who have left the school are removed from the system.

If anyone thinks their password may have been compromised or someone else has become aware of the password, this must be reported to the Head Teacher /Network Manager.

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.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's Online e-Safety Policy and Data Security.
- Users are provided with an individual network, email, learning platform and Management Information System log-in username. From **Year 9** they are also expected to use a personal password and keep it private.
- Pupils are not permitted to deliberately access on-line materials or files on the school network or local storage devices 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 periodically. Individual staff users must also make sure that workstations are not left unattended and are locked.
- Due consideration should be given when logging into the school learning platform, virtual learning environment or other online application to the browser/cache options (shared or private computer).
- In our school, all ICT password policies are the responsibility of **Justine Golamhossen**

and all staff and pupils are expected to comply with the policies at all times.

ZOMBIE ACCOUNTS

'Zombie accounts' refers to accounts belonging to users who have left the school and therefore no longer have authorised access to the school's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.

- Ensure that all user accounts are disabled once the member of the school has left.
- Prompt action on disabling accounts will prevent unauthorised access.
- Regularly change generic passwords to avoid unauthorised access.

PERSONAL OR SENSITIVE INFORMATION

PROTECTING PERSONAL, SENSITIVE, CONFIDENTIAL AND CLASSIFIED INFORMATION

- Ensure that any school information accessed from a personal PC or removable media equipment is kept secure and any portable media is removed from computers when not attended.
- Ensure screens are locked before moving away from computers during a normal working day to prevent unauthorised access.
- Ensure the accuracy of any personal, sensitive, confidential, and classified information that is disclosed or shared 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 that is copied, scanned, or printed. This is particularly important when shared copiers (multi-function print, scan, and copiers) are used and when access is from a non-school environment.
- Only download personal data from systems if expressly authorised to do so by the Head Teacher / Principal.
- Personal, sensitive, confidential, or classified information must not be posted on the internet, or such information disseminated in any way that may compromise its intended restricted audience.
- Screen displays must be kept out of direct view of any third parties when accessing personal, sensitive, confidential, or classified information.
- Hard copies of data must be securely stored and disposed of after use in accordance with the document labeling.

STORING/TRANSFERRING PERSONAL, SENSITIVE, CONFIDENTIAL OR CLASSIFIED INFORMATION USING REMOVABLE MEDIA

- Removable media should be purchased with encryption.
- All removable media must be stored securely.

- All removable media that may hold personal data must be securely disposed of.
- All files containing personal, sensitive, confidential, or classified data must be encrypted.
- Hard drives from machines no longer in service must be removed and stored securely or wiped clean.

Guidance on How to Encrypt Files can be found on the ICO website:

<https://ico.org.uk/media/for-organisations/encryption-1-0.pdf>

REMOTE ACCESS Staff members are responsible for all activity via their remote access facility.

- Any equipment must be used with an appropriate level of security for remote access.
- To prevent unauthorised access to school systems, all dial-up access information such as telephone numbers, logon IDs and PINs must be kept confidential and not disclosed to anyone.
- PINs must be selected to ensure that they are not easily guessed, e.g., do not use personal house or telephone number or choose consecutive or repeated numbers.
- Writing down or otherwise recording any network access information must be avoided. 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.
- School information and data must be protected, including any printed material produced while using the remote access facility. Particular care must be taken when access is from a non-school environment.

SAFE USE OF IMAGES

TAKING OF IMAGES AND FILM

The following applies to all parts of the school including Pre-School and ABCs (EYFS).

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- The school permits the appropriate taking of images by staff and pupils with school equipment with the written consent of parents (on behalf of pupils) and staff.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips except with the express permission of the Headteacher provided they are transferred immediately and solely to the school's network and deleted from the staff device.
- Students 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 Head Teacher.
- Pupils and staff must have permission from the Headteacher before any image can be uploaded for publication.

CONSENT OF ADULTS WHO WORK AT THE SCHOOL

- Permission to use images of all staff who work at the school is sought on induction and a copy to be located in the personnel file.

PUBLISHING PUPIL'S IMAGES AND WORK

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

- on the school website.
- in the school prospectus and other printed publications that the school may produce for promotional purposes.
- recorded/ transmitted on a video or webcam.
- on the school's learning platform or Virtual Learning Environment,
- 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 this 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. Consent must also be given in writing and will be kept on record by the school.

Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names 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.

Only the ICT Manager or Justine Golamhossen has authority to upload to the internet.

STORAGE OF IMAGES

- In line with UK GDPR images are used only with the written consent of parents/carers which is secured in the first instance on a child's entry to the school. Records are kept on file and consent can be changed by parents/carers at any time.
- Images/ films of children are stored on the school's network.
- Students and 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 teaching staff and pupils within the confines of the school network or other online school resource.
- **Justine Golamhossen** has the responsibility of deleting the images when they are no longer required, or when the pupil has left the school.

WEBCAMS AND CCTV

- The school may use CCTV for security and safety.
- Notification of CCTV use will be displayed at the front of the school. Please refer to the hyperlink below for further guidance <https://ico.org.uk/media/about-the-ico/consultations/2044/draft-cctv-cop.pdf>
- We do not use publicly accessible webcams in school.
- Webcams will not be used for broadcast on the internet without prior parental consent.
- Misuse of the webcam by any member of the school community will result in sanctions (as listed under the 'inappropriate materials' section of this document).
 - Notification is given in this/these area(s) filmed by webcams by signage.
 - Consent is sought from parents/carers and staff on joining the school, in the same way as for all images.
- Webcams include any camera on an electronic device which is capable of producing video. School policy should be followed regarding the use of such personal devices.

VIDEO CONFERENCING

- Permission is sought from parents and carers if their children are involved in video conferences with endpoints outside of the school.
- All pupils are supervised by a member of staff when video conferencing.
- The school keeps a record of video conferences, including date, time, and participants.
- Approval from the Headteacher is sought prior to all video conferences within school to end-points beyond the school.
- The school conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences.
- No part of any video conference is recorded in any medium without the written consent of those taking part.

Additional points to consider:

- Participants in conferences offered by 3rd party organisations may not be DBS checked.
- Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference.

SCHOOL ICT EQUIPMENT INCLUDING PORTABLE & MOBILE ICT EQUIPMENT AND REMOVABLE MEDIA

SCHOOL ICT EQUIPMENT

- As users of the school ICT equipment, all staff are responsible for their own activity.

- Any ICT equipment issued to staff is logged and serial numbers recorded as part of the school's inventory.
- Visitors should not plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT facilities if available.
- All ICT equipment is kept physically secure.
- Unauthorised access or unauthorised modifications should not be made to computer equipment, programs, files, or data. This is an offence under the Computer Misuse Act 1990.
- All data should be saved on a frequent basis to the school's network. Staff are responsible for the backup and restoration of any data that is not held on the school's network.
- Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick or another portable device. If it is necessary to do so the local drive must be encrypted.
- It is recommended that a time locking screensaver is applied to all machines. Any device accessing personal data must have a locking screensaver as must any user profiles.
- Privately owned ICT equipment should not be used on a school network.
- On termination of employment, resignation, or transfer, all school ICT equipment should be returned to the school. Details of all system logons must be provided to the school so that they can be disabled.
- It is the responsibility of each staff member to ensure that any information accessed from their own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential, or classified information is disclosed to any unauthorised person.
- All ICT equipment allocated to staff must be authorised by the Headteacher
 - maintaining control of the allocation.
 - recovering and returning equipment when no longer needed.
- All redundant ICT equipment will be disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA).

PORTABLE & MOBILE ICT EQUIPMENT

This section covers such items as laptops, mobile devices, and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data.

- All activities carried out on school systems and hardware will be monitored in accordance with the general policy.
- Staff must ensure that all school data is stored on the school network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted.
- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of the car before starting a journey.

- All locally stored data, including diary entries, must be synchronised with the central school network server on a frequent basis.
- Portable and mobile ICT equipment should be made available as necessary for anti-virus updates and software installations, patches, or upgrades.
- The installation of any applications or software packages must be authorised by the ICT support team, fully licensed, and only carried out by the ICT support.
- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight.
- Portable equipment must be transported in its protective case if supplied.

MOBILE TECHNOLOGIES

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Mobile technologies such as smartphones, tablets, and games players, are generally very familiar to children outside of school. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

PERSONAL MOBILE DEVICES (INCLUDING MOBILE PHONES)

- The school allows staff to bring in personal mobile phones and devices for their own use. 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 not use them for personal purposes within lesson time. At all times the device must be switched onto silent.
- This technology may be used for educational purposes, as mutually agreed with the Headteacher. The device user, in this instance, must always ask the prior permission of the bill payer.
- 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.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- Never use a hand-held mobile phone whilst driving a vehicle.

SCHOOL PROVIDED MOBILE DEVICES (INCLUDING MOBILE PHONES)

- The school does not provide any mobile devices.

TELEPHONE SERVICES

- Personal telephone calls may be made or received, provided:
 1. They are infrequent, kept as brief as possible and do not cause annoyance to others.
 2. They are not for profit or to premium rate services.
 3. They conform to this and other relevant school policies.
- Be aware that the laws of slander apply to telephone calls. Whilst a telephone call may seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases.
- Ensure that any incoming telephone calls can be handled at all times.
- Follow the appropriate procedures in the event of receiving a telephone call containing a bomb threat. These procedures are readily available from the office.

REMOVABLE MEDIA

If storing or transferring personal, sensitive, confidential, or classified information using Removable Media please refer to the section: **Ensure** screens are locked before moving away from computers during a normal working day to prevent unauthorised access.

Ensure the accuracy of any personal, sensitive, confidential, and classified information that is disclosed or shared 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 that is copied, scanned, or printed. This is particularly important when shared copiers (multi-function print, scan, and copiers) are used and when access is from a non-school environment.
- Only download personal data from systems if expressly authorised to do so by the Head Teacher / Principal.
- Personal, sensitive, confidential, or classified information must not be posted on the internet, or such information disseminated in any way that may compromise its intended restricted audience.
- Screen displays must be kept out of direct view of any third parties when accessing personal, sensitive, confidential, or classified information.
- Hard copies of data must be securely stored and disposed of after use in accordance with the document labeling.

STORING/TRANSFERRING PERSONAL, SENSITIVE, CONFIDENTIAL OR CLASSIFIED INFORMATION USING REMOVABLE MEDIA'

- Always consider if an alternative solution already exists.
- Only use recommended removable media.
- Encrypt and password protect.
- Store all removable media securely.

Removable media must be disposed of securely by the ICT manager.

SOCIAL MEDIA

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

- Our school may Facebook and Twitter to communicate with parents and carers. Justine Golamhossen is responsible for all postings on these technologies and monitors responses from others.
- Staff are not permitted to access their personal social media accounts using school equipment at during school hours.
- Staff are able to setup Social Learning Platform accounts, using their school email address, in order to be able to teach pupils the safe and responsible use of social media.
- Students are not permitted to access their social media accounts whilst at school.
- Staff, Governors, students, parents, and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others.
- Staff, Governors, pupils, parents, and carers are aware that the information, comments, images, and video they post online can be viewed by others, copied, and stay online forever.
- Staff, Governors pupils, parents, and carers are aware that their online behaviour should always be compatible with UK law.

SYSTEMS AND ACCESS

- Staff are responsible for all activity on school systems carried out under any access/account rights assigned to them, whether accessed via school ICT equipment or their own PC or laptop.
- Unauthorised persons must not be allowed to use school ICT facilities and services that have been provided to staff.
- All portable media must be removed from computers when they are left unattended.
- Only personal logons, account IDs and passwords should be used and not used by anyone else.
- Screen displays must be kept out of direct view of any third parties when accessing personal, sensitive, confidential, or classified information.
- Screens should be locked before moving away from computers during the normal working day to protect any personal, sensitive, confidential, or otherwise classified data and to prevent unauthorised access.
- Staff must logoff from the computer completely when being away from it for a longer period of time.
- Viruses must not be introduced or propagated.
- It is imperative that staff do not access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libelous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring

the school 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 (in accordance with the Sex Discrimination Act, the Race Relations Act, and the Disability Discrimination Act).

- Any information held on School systems, hardware or used in relation to School business may be subject to The Freedom of Information Act.
- Where necessary, permission must be obtained from the owner or owning authority and any relevant fees paid before using, copying, or distributing any material that is protected under the Copyright, Designs and Patents Act 1998.

It is essential that any hard drives which may have held personal or confidential data are 'scrubbed' in way that means the data can no longer be read. It is not sufficient to simply delete the files or reformat the hard drive. Whoever is appointed to dispose of the equipment must provide a **written guarantee** that they will irretrievably destroy the data by multiple over writing the data.

WRITING AND REVIEWING THIS POLICY

STAFF AND PUPIL INVOLVEMENT IN POLICY CREATION

Staff, Governors and students have been involved in reviewing the ICT Acceptable Use Agreements through the School Council and Staff Meetings.

REVIEW PROCEDURE

There will be on-going opportunities for staff to discuss with the e-Safety coordinator any e-Safety issue that concerns them.

There will be on-going opportunities for staff to discuss with the AIO any issue of data security that concerns them.

This policy will be reviewed regularly (expect every 24 months) and consideration will be given to the implications for future whole school development planning.

The policy will be amended if new technologies are adopted, or Central Government change the orders or guidance in any way.

This policy has been read, amended, and approved by the Headteacher, the Deputy Head and the Safeguarding Governor.

Brenda Lewis

December 2023

ACCEPTABLE USE AGREEMENTS

Student Acceptable Use Agreement / E-Safety Rules – Each student should receive a copy to read

Primary Pupil Acceptable Use Agreement / e-Safety Rules – All parents/carers should read these with primary age children and sign to say they agree

Senior Pupil Acceptable Use Agreement / e-Safety Rules – Students at this age can sign these for themselves

Parent/Carer Acceptable Use Agreement / Code of Conduct – All parents/carers should read and sign this document

Staff, Volunteer and Visitor Acceptable Use Agreement / E-Safety / Code of Conduct – All staff, volunteers and visitors should read and sign this document.

King of Kings School

Student Acceptable Use Agreement / E-Safety Rules

You should:

- **Only access the internet under the direct supervision of a member of staff, and never access the internet when a member of staff is not present in the same room.**
- Only access sites which are appropriate for use in school. Personal websites (e.g., Facebook, Instagram, Tumblr, Tic Tok, etc.) are **not** appropriate for use in school.
- Be aware that your actions on the Internet can be seen by others.
- Treat others as they would expect to be treated, e.g., show respect and be polite.
- Be aware that information on an Internet website may be inaccurate or biased. Try to verify the information using other sources, if possible, before using it.
- Respect copyright and trademarks. You must not copy text or pictures from the Internet and hand it in to your teacher as your own work.
- Always tell your teacher or another adult if you ever see, hear, or read anything which makes you feel uncomfortable while using the Internet or e-mail.
- Always check with a supervisor before taking the following actions:
 - downloading files;
 - completing questionnaires or subscription forms;
 - opening e-mail attachments.

You must NOT:

- Access chat rooms/personal websites.
- Use or send bad, threatening, or annoying language.
- Post anonymous messages or forward chain letters.
- Use school computers for gambling, political purposes, or advertising.
- Interfere with another student's work.
- Intentionally waste resources.
- Access or send inappropriate materials such as pornographic, racist, or offensive material.
- Access games – unless given express permission by the Headteacher/Deputy Head.

Please note:

- You should always log out when your session has finished.
- All computers will be closely monitored, and staff may review your files and communications to maintain system integrity.
- All Internet activity should be appropriate to your education.
- Failure to follow the code will result in loss of access and further disciplinary action may be taken if appropriate.

King of Kings school
Primary Pupil Acceptable Use Agreement / e-Safety
Rules

- I will only use ICT in school for school purposes.
- I will only use my class e-mail address or my own school e-mail address when e-mailing for school related work.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will not tell other people my ICT passwords.
- I will only open or delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite, and sensible.
- I will not look for, save, or send anything that could be unpleasant or nasty. If I accidentally find anything like this, I will tell my Supervisor/Teacher immediately.
- I will not give out my own or others' details such as name, phone number, or home address.
- I will not arrange to meet someone or send my image unless this is part of a school project approved by my Supervisor/Teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will support the school approach to online safety and not upload or add any images, video, sounds, or text that could upset any member of the school community or wider community.
- I know that my use of ICT can be checked, and my parent/carers contacted if a member of school staff is concerned about my safety.
- I will not sign up for any online service unless this is an agreed part of a school project approved by my Supervisor/Teacher.
- I will not bring a Smart Watch to school because I am not allowed to wear one during the school day.
- I will not sign up to online services until I am old enough.

Signature(Parent /Carer) Date

Full Name (Printed)

To be read by the parent with the student and signed by the parent

King of Kings School

Senior Pupil Acceptable Use Agreement /e-Safety Rules

- I will only use ICT systems in school, including the internet, e-mail, digital video, and mobile technologies for school purposes.
- I will not download or install software on school technologies.
- I will only log on to the school network, other systems, and resources with my own username and password.
- I will follow the school's ICT security system and not reveal my passwords to anyone and change them regularly.
- I will only use my school e-mail address for school related work.
- I will make sure that all ICT communications with pupils, Supervisors/Teachers, or others is responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not browse, download, upload, or forward material that could be considered offensive or illegal. If I accidentally come across any such material, I will report it immediately to my Supervisor/Teacher.
- I will not give out any personal information such as name, phone number, or address.
- I will not arrange to meet someone unless this is part of a school project approved by my Supervisor/Teacher.
- I am aware that when I take images of pupils and/or staff that I must only store and use these for school purposes in line with school policy and must never distribute these outside the school network without the permission of all parties involved. This includes school breaks and all occasions when I am in school uniform or when otherwise representing the school.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils, or others distress or bring the school community into disrepute, including through uploads of images, video, sounds, or texts.
- I will support the school approach to online safety and not upload or add any images, video, sounds or text that could upset any member of the school community or wider community.
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my Supervisor/Teacher.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied, and my parent/carer may be contacted.
- I will not bring a Smart Watch to school because I am not permitted to wear one during the school day.
- I will not sign up to online services until I am old enough to do so.

Signature Date *To be signed by the student*

Full Name (Printed)

King of Kings School

Parent/Carer

Acceptable Use Agreement / Code of Conduct

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should always have an entitlement to safe internet access.

This Acceptable Use Agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal, and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people regarding their on-line behaviour.

The King of Kings School will do their best to ensure that students will have good access to ICT to enhance their learning and will, in return, expect the students to agree to be responsible users. A copy of the Student Acceptable Use Agreement is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent/Carer's Name

Student Name

As the parent/carers of the above student, I give permission for them to have access to the internet and to ICT systems at school.

I/We have discussed this document with _____ (Child's name) and know that they have signed an Acceptable Use Agreement and we agree to follow the e-Safety rules and to support the safe use of ICT at the King of Kings School.

I/We know they have received, or will receive, e-safety education to help them understand the importance of safe use of ICT – both in and out of school.

I/We understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that all students within this school will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I/We understand that my/our child's activity on the ICT systems will be monitored and that the school will contact me/us if they have concerns about any possible breaches of the Acceptable Use Agreement.

I/We will encourage my/our child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

- I/We will support the school's approach to online safety and not upload or add any

text, image, sound, or videos that could upset or offend any member of the school community or bring the school name into disrepute.

- I/We will ensure that my/our online activity will not cause the school, staff, pupils, or others distress or bring the school community into disrepute.
- I/We will close online accounts if I/we/Supervisors/Teachers find that these accounts are active for our underage child/children.
- I/We agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school.

Signature Date

Full Name (Printed)

Child's Name

Relationship to child

Signature Date

Full Name (Printed)

Child's Name

Relationship to child

Please return this agreement to the school.

Tick here if you would like a copy for your personal records

☐

King of Kings School

Staff, Volunteer, and Visitor Acceptable Use Agreement / E-Safety / Code of Conduct

Introduction

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This agreement is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this agreement and adhere at all times to its contents. Any concerns or clarification should be discussed with [Name of Staff](#).

This Acceptable Use Agreement is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal, and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.
- that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for students learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I will follow requirements for data protection as outlined in the Online e-Safety and Data Protection Policy.
- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g., laptops, email, etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology 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.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- 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 / video images. I will not use my personal equipment to record these images unless I have permission to do so. Where these images are published (e.g., on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- Photographs will be kept securely and used appropriately, whether in school, taken off the school premises, or accessed remotely.
- Images of pupils and/ or staff will only be taken, stored, and used for professional purposes in line with school policy and with written consent of the parent, carer, or staff member.
- Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher
- I will support the school approach to online safety and not upload or add any images, video, sounds, or text linked to or associated with the school or its community.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with students/pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- Staff should be made aware of the risks attached to using their personal email addresses / mobile phones / social networking sites for such communications
- I will not engage in any on-line activity that may compromise my professional responsibilities.

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

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses.
- I will not give out my own personal details, such as mobile phone number, personal e-mail address, personal Twitter/Facebook/Tic Tok/Instagram account, or any other social media link, to pupils.
- I will not open any hyperlinks in emails or any attachments in emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- 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.
- 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 allowed. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that the Data Protection Policy requires that any staff or student 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 school 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 the school:

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

User Signature

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines, and agree to the above Acceptable Use Agreement / E-Safety Rules

I understand this forms part of the terms and conditions set out in my contract of employment and agree to follow this code of conduct

Signature Date

Full Name (Printed)

Job title

HELP AND SUPPORT

See Manchester Safeguarding Children Partnership for local advice

Our organisation has a legal obligation to protect sensitive information under the Data Protection Act 2018. For more information visit the website of the Information Commissioner's Office <https://ico.org.uk/>

The Information Management Toolkit for Schools is available at:

<https://irms.org.uk/general/custom.asp?page=SchoolsToolkit>

Safeguarding Children online – free expert advice: <http://www.getsafeonline.org>

Review Online e-Safety Policy and practice at <https://360safe.org.uk/>

Data Protection Team – email dele@deleoye.com

Resources to support schools with online safety:

- [/UKCIS Education for a Connected World.pdf/](#)
- Guidance from the PSHE Association
- [Internet Legends by Parent Zone & Google](#)
- Organisations are listed in Annex D of KCSIE, that can provide support concerning online safety.

CURRENT LEGISLATION

ACTS RELATING TO MONITORING OF STAFF EMAIL

Data Protection Act 2018

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individual's rights of access to their personal data, compensation, and prevention of processing. The **Data Protection Act 2018** implements the UK General Data Protection Regulation (GDPR) in national law.

<http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

<http://www.hms0.gov.uk/si/si2000/20002699.htm>

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

<https://www.legislation.gov.uk/ukpga/2000/23>

Human Rights Act 1998

<https://www.legislation.gov.uk/ukpga/1998/42>

OTHER ACTS RELATING TO ESAFETY

Racial and Religious Hatred Act 2006

It is a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing, or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality, or ethnic background.

<http://www.legislation.gov.uk/ukpga/2006/1>

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos, or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of *Working Together to Safeguard Children, 2018* document as part of their child protection packs.

<https://www.legislation.gov.uk/ukpga/2003/42>

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene, or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent there is no need to prove any intent or purpose.

<http://www.legislation.gov.uk/ukpga/2003/21/section/127>

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another person's password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

<https://www.legislation.gov.uk/ukpga/1990/18>

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

<https://www.legislation.gov.uk/ukpga/1988/27>

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film, and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining their author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

<https://www.legislation.gov.uk/ukpga/1988/48>

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing, or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

<https://www.legislation.gov.uk/ukpga/1986/64>

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

<https://www.legislation.gov.uk/ukpga/1978/37>

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

<https://www.legislation.gov.uk/ukpga/Eliz2/7-8/66> and
<http://www.legislation.gov.uk/ukpga/1964/74>

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

<https://www.legislation.gov.uk/ukpga/1997/40>

ACTS RELATING TO THE PROTECTION OF PERSONAL DATA

Data Protection Act 2018

<http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>

The Freedom of Information Act 2000

<https://www.legislation.gov.uk/ukpga/2000/36>
<https://ico.org.uk/for-organisations/guide-to-freedom-of-information/>

COUNTER-TERRORISM AND SECURITY ACT 2015 (PREVENT), ANTI-RADICALISATION & COUNTER-EXTREMISM GUIDANCE

<https://www.gov.uk/government/publications/preventing-extremism-in-schools-and-childrens-services>

The school holds the document ‘*The Prevent duty Departmental Advice for Schools and Childcare Providers, June 2015*’ on file.