KNIGHTSBRIDGE SCHOOL

ICT and e-Safety Policy

1. Introduction and Overview

This policy needs to be read in conjunction with:
Home-School Contract for the Safe use of The Internet and Digital Technologies, Pupil ICT Acceptable Use Policy, Behaviour and Discipline Policy, Anti-Bullying Policy (including cyber-bullying), Complaints Policy, Safeguarding Child Protection Policy, and Staff Code of Conduct, KS Policy for Distance Teaching and Learning; Safeguarding - Child Protection Policy and The Peer-on-Peer Abuse policy.

Rationale

In relation to the digital technologies and internet services at Knightsbridge School the purpose of this policy is to:

- Set out the key principles for the safe and responsible use
- Safeguard and protect children and staff
- Staff need to be aware of the systems in place, manage them effectively
- Help staff understand the risks, demonstrate best practices and to monitor their own standards
- Know how to escalate concerns when identified
- Set clear expectations for appropriate behaviour and codes of practice
- Have clear structures to deal with the issues and threats that may arise and to cross reference with other school policies
- Ensure that all members of the school community are aware that unsafe or unlawful behaviour is unacceptable and that when appropriate, disciplinary or legal action may be taken
- Minimise the risk of misplaced or malicious allegations made against adults who work with pupils
- Minimise the risk of radicalisation under the Prevent Duty (2015).

The main risks to our school community are summarised as follows:

- Identity theft including hijacking others accounts or online profiles
- Inappropriate use or disclosure of personal information
- Health and well-being, including the amount of time spent online
- Sending and receiving of personal images or data
- Lack of care or consideration for the intellectual property of others – including software, text, images, music and film
- Not verifying the authenticity or accuracy of online content
- Ignorance of one's digital footprint and online reputation
- Cyberbullying
- Online grooming
- Risk of radicalisation and/or access to electronic information that may lead to indoctrination into any form of extreme ideology.

While internet access is appropriately filtered and monitored, we acknowledge that technical solutions are not perfect and so there is always a small risk of exposure to inappropriate and age inappropriate content.

Scope

This policy applies to all members of the Knightsbridge School community including staff, pupils, volunteers, parents/guardians and visitors who have access to the school and its ICT systems.

The Education and Inspections Act 2006 empowers Heads to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyberbullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for, and of, electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the school's Safeguarding; Child Protection Policy, Peer-on-Peer Abuse policy and Behaviour Policy. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/guardians of incidents of inappropriate e-safety behaviour that take place out of school. The school take seriously its responsibilities under the Counter Terrorism and Security Act (2015) including the Prevent Duty and the measures in this policy are consistent with these.

Roles and responsibilities

Role	Key Responsibilities
SLT (Principal, Head and Bursar)	● Take overall responsibility for e-safety provision while the day to day responsibility is delegated to the e-Safety Officer ● Ensures the school has invested in and maintains appropriate IT systems and the expertise to support the e-safety provisions ● Are responsible for ensuring that the e-Safety Officer and other staff receive suitable training to carry out their e-safety roles and to train other colleagues, as necessary ● To be aware of procedures to be followed in the event of a serious e-safety incident. ● Ensure that the relevant systems are in place to support staff who carry out internal e-safety procedures (e.g. Network Manager, Helpdesk Technician, Head of IT) ● Support the effort to promote and raise awareness of e-safety awareness with parents and the wider school community
e-Safety Officer	● Takes day to day responsibility for e-safety issues across the school

- Has a leading role in establishing and reviewing the school ICT and e-safety Policies and documents
- Promotes an awareness and commitment to e-safeguarding throughout the school community
- Oversees the delivery of the e-safety element of the Computing curriculum
- Ensures that e-safety education is embedded across the curriculum
- Liaises with school technical IT staff on e-safety and IT security Matters
- Communicates regularly with SLT to discuss current issues and trends
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident
- Facilitates e-safety training and advice for all staff
- Liaises with the school's Designated Safeguarding Lead (DSL)
- Is regularly updated in e-safety issues and legislation, and is aware of the potential for serious child protection issues that can arise from:
    - sharing of personal data
    - access to illegal / inappropriate materials
    - inappropriate on-line contact with adults / strangers
    - potential or actual incidents of grooming
    - cyber-bullying and use of social media

Proprietor/Advisors

- Ensure that the school follows all current and relevant e-safety advice to keep children and staff safe
- Approve the school's e-safety Policy and review the effectiveness of it
- Support the school in encouraging parents and the wider community to become engaged with e-safety

IT Team

- Report any e-safety related issues that arise to the designated e-safety Officer
- Ensure provision exists for monitoring and detection of misuse or malicious attack
- Ensure that appropriate ICT access controls exist to protect pupil data, personal and sensitive information held by the school
- Ensure the school effectively applies internet content filtering and that it is reviewed on a regular basis
- That he/she keeps up to date with the school's e-safety Policy and technical information in order to effectively carry out their duties and to inform and update others as relevant

	● The use of the school's IT systems and services are monitored in order that any misuse or attempted misuse can be identified and investigated further ● Ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster ● To keep up-to-date documentation of the school's ICT system and services ● Ensure that users may only access the school's networks through an authorised and properly enforced password protection policy ● Liaises with DSL & teacher of Computing on e-safety and security matters.
Teachers	● Demonstrate the principles of e-safety in their professional practice ● Embed e-safety in all relevant aspects of the curriculum and other school activities ● Supervise and guide pupils carefully when engaged in activities involving digital technology (including extra-curricular and extended school activities) ● Help pupils build critical research skills by cross referencing sources and to disregard false news and information ● Encourage pupils to develop research skills and awareness of the legal issues relating to electronic content such as copyright laws and plagiarism
All staff	● Read, understand, sign and adhere to the school's Staff ICT Acceptable Use Policy ● Read, understand and help promote the school's e-safety policies and guidance and guidance as set out in Knightsbridge School – Distance Teaching and Learning. ● Ensure KS Behaviour Policy Appendix A3 is applied in cases of misuse. ● Be aware of e-safety issues related to the use of mobile phones, cameras and handheld devices and that they monitor their use and implement current school policies with regard to these devices ● Report any suspected misuse, concern, incident or problem to the designated e-safety Officer ● Maintain an awareness of current e-safety issues and guidance, and attending relevant INSET in this area ● Model safe, responsible and professional behaviours in their own use of technology ● Ensure that any digital communications with pupils should be on a professional level and only through school based systems, never

	through personal mechanisms, such as personal email, text, or own smart phones
Pupils	● Read, understand, sign and adhere to the relevant Pupil ICT Acceptable Use Policy ● Y4-Y9 read and have a good understanding of the KS Remote Learning Guidance for Parents and Pupils in the Senior School. ● Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations ● Understand the importance of reporting abuse, misuse or access to inappropriate materials ● Know what action to take if they or someone they know feels worried or vulnerable when using online technology ● Know and understand school policy on the use of laptops, tablets, mobile phones, digital cameras and handheld devices ● Know and understand school policy on the taking or use of images of others and on cyber-bullying ● Understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's e-safety Policy covers their actions out of school, if related to their membership of the school. ● Take responsibility for learning about the benefits and risks of using the Internet and other technologies safely, both in school and at home. ● Where email accounts are activated in S5-S9, these are used solely in the communication between Knightsbridge users. Pupils are also expected to follow netiquette guidelines provided. ● Understand the need to cross reference online content so to identify and disregard false news and information
Parents/Guardians	● Read, understand and sign the Home-School Contract for the Safe use of The Internet and Digital Technologies. ● To understand what system are in place to filter and monitor online use ● Support the school's commitment to e-safety by reinforcing the principles of e-safety at home and outside of school ● Access and use the school website, parent portal and any other school systems made available to parents in accordance with the relevant school Acceptable Use Agreement ● Consult with the school if they have any concerns about their children's use of technology or the use of ICT in a school context ● To be made aware of who your child is going to be interacting with online

External individuals or contractors	● Any external individual/organisation that needs access to schools ICT systems or services to carry out their duties on behalf of the school will obtain prior approval and abide by the appropriate Acceptable Use Policy.

Communication

How the policy will be communicated to staff/pupils/community in the following ways:

- The policy is posted in the policies section of the 'teachers read' drive and on the Parent portal
- The policy is included in the school induction pack for new staff
- e-safety and the appropriate use of ICT is embedded in the curriculum at all stages in the school
- Home-School Contract for the Safe use of The Internet and Digital Technologies are issued to the whole school's parent community, usually on entry to the school, or when significant revisions have been made
- Acceptable use agreements are issued to the whole school's pupil community at the start of each new school year or when significant revisions have been made

Complaints handling

The school will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on school devices or systems. Neither the school, the schools directors, employees or contractors can accept liability for material accessed, or any consequences arising from its access.

Staff and pupils are given information about infringements in the use of ICT and the possible interventions or sanctions. Appendix A3 of the school's Behaviour Policy outlines specific behaviours and consequences. For pupils sanctions include but are not limited to:

- Interview or counselling by their class teacher/tutor, designated e-safety Officer or appropriate member of the SLT;
- Informing parents or guardians;
- Removal of internet or computer access for a period, which could ultimately prevent access to files held on the system, including those for external examination or coursework
- Referral to the appropriate local authorities and Police.

For staff, infringements to the school's acceptable use of ICT or e-safety policy will be assessed by the Head or other member of the senior leadership team and when deemed appropriate, and will be dealt with under the school's disciplinary procedures.

Our designated e-safety Officer acts as the first point of contact for any complaint. Any complaint about staff misuse is referred to the Head.

Complaints of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school's safeguarding procedures and Complaints Policy.

Review and Monitoring

- The ICT & e-safety Policy is referenced from within other school policies as noted at the start of this document
- The designated e-safety Officer will be responsible for the document review and updates in collaboration with the schools Network Manager, Head of Computing and the SLT
- The ICT & e-safety Policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school or technologies that become popular with members of the school community, or changes in legislation

2. Education and Curriculum

Pupil e-safety curriculum

This school

- Has a clear, progressive e-safety education programme as part of the Digital Technology curriculum. It covers a range of skills and behaviours appropriate to their age and experience, including:
    - to STOP and THINK before they CLICK
    - to develop a range of strategies to evaluate and verify information before accepting its accuracy
    - to be aware that the author of a website, or a comment on a webpage, may have a particular bias or purpose and to develop skills to recognise what that may be
    - to know how to narrow down or refine an internet search
    - to understand how search engines work and to understand that this affects the results they see at the top of the listings
    - to understand acceptable behaviour when using online services, i.e. be polite, never use bad or abusive language or other inappropriate behaviour; keep personal information private
    - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention
    - to understand why online 'friends' may not be who they say they are and to understand why they should be careful in online environments
    - to understand the risks posed by adults or young people who use the Internet and social media to bully, groom, abuse or radicalise other people
    - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings
    - to understand why they must not post pictures or videos of others without their permission
    - to know not to download files, such as programs, apps. videos or music, without permission

    - to have strategies for dealing with the receipt of inappropriate materials
    - to understand why and how some people will 'groom' young people for sexual reasons
    - to understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying
    - to know how to report any peer-on-peer abuse including cyberbullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent or guardian, teacher or trusted staff member, or an organisation such as Childline or CEOP
    - to understand that their accounts are for their own use and logging in to other users accounts is never acceptable

- Plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas
- Will remind pupils about their responsibilities through The Pupil ICT Acceptable Use Policy which every pupil will agree to
- Ensures that when copying materials from the web, pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright or intellectual property rights
- Ensures that pupils understand the importance of the safe use of digital technology and the Internet and adjust their behaviour in order to reduce risks and build resilience to threats including radicalisation
- Ensure that within their distance learning, pupils follow netiquette guidelines and make use of media & resources as directed by teachers.

Staff training

This school:

- Ensures staff know how to handle data and when to encrypt data especially when:
    - Sending or receiving sensitive and personal information, and
    - Sensitive or personal information is taken off site
    - Using personal or home computing devices
- Makes training available to staff on e-safety issues as part of the school's e-safety education program
- Provides, as part of the induction process, all new staff and outside parties who access the school ICT systems with information and guidance on the ICT & e-safety Policy and the school's Acceptable Use Policies
- Provides training for all staff on the use of G Suite for Education as a platform for remote learning.
- Encourages staff to model safe and responsible behaviour in their own use of technology in and out of school
- Educates staff in the need to use strong passwords for all school systems and their own personal accounts and to always keep their second factor security key available, safe and secure.

Parent awareness and training

This school

- Aims to run a rolling programme of advice, guidance and training for parents, including:

- Agreement to the *Home-School Contract for the Safe use of The Internet and Digital Technologies*, to ensure that principles of e-safety are made clear and promoted both in and out of school
- Parent seminars, demonstrations, or practical sessions held at school
- Suggestions for safe Internet use at home
- Provision of information about national support sites for parents
- KS Remote Guidance for Parents and Pupils in the Junior and Senior School

3. Expected Conduct and Incident Management

Expected conduct

In this school, all users:

- Are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign and agree to before being given access to school systems
- Need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- Need to understand the importance of reporting peer-on-peer abuse, misuse or access to inappropriate materials and know how to do so
- Should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's ICT & e-safety Policy covers their actions out of school, if related to their membership of the school
- Will be expected to know and understand, on an age appropriate basis, the school's policies on the use of mobile phones, digital cameras and handheld devices. They should also know and understand school policies on the taking/use of images and on cyberbullying

Incident management

In this school:

- We embed the principles of the ICT & e-safety Policy in our day to day work and there is a differentiated and appropriate range of sanctions available to address infringements when it is appropriate to do so
- All members of the school and its wider community are encouraged to be vigilant in reporting e-safety issues, in the confidence that issues will be dealt with quickly and sensitively, through the procedure set out in our Complaints Policy
- Support is sought from other agencies as needed in dealing with e-safety issues
- Monitoring and reporting of e-safety incidents takes place and contributes to developments in policy and practice in e-safety within the school. The records are reviewed/audited and reported to the SLT and Directors as required
- We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law

4. Managing the ICT infrastructure

Internet access, security and content filtering

This school:

- Provides appropriately secure environments for pupils to publish material safely
- Requires staff to preview websites and content before they are used for teaching, classroom or school activities
- Ensures staff are vigilant when conducting text, image or video searches on the Internet in the presence of pupils
- Informs all users that Internet use is monitored
- Informs staff and pupils that that they must report any failure of the filtering systems directly to the designated e-safety Officer or member of the IT team
- Makes clear all users know and understand what is 'appropriate use' and what sanctions result from misuse
- Provides guidance for the reporting of offensive materials, peer-on-peer abuse, or bullying etc.
- Has perimeter network security in place to monitor all inbound and outbound Internet traffic and scan and block inappropriate content and to protect the school network from malicious activities and threats
- Uses group-level policies to tailor Internet access to different user groups
- Uses end-point security software to protect school computers from viruses & threats
- Uses encrypted devices and secure remote access in the event staff need to access confidential data off-site
- Blocks popular social networking sites, forums and chat except those that are part of a teacher led activity
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes
- Is vigilant in its supervision of pupils' ICT use, as far as is reasonable, and uses common-sense strategies to manage pupil access to online content
- Ensures all staff and pupils have signed the school ICT acceptable use agreement and understands that they must report any concerns to the designated e-safety Officer, form tutor or member of the SLT
- Refers any material we suspect is illegal to the appropriate authorities such as the Police and the Local Authority

Network management

This school:

- Uses individual password protected accounts for all members of the school community
- Issues physical security keys for second factor authentication of staff Google Workspace accounts
- Uses limited guest accounts occasionally for external or short term visitors for temporary access to appropriate services
- Uses remote management tools for controlling/viewing users/setting-up computers
- Stores confidential data on school systems or cloud services within the bounds of current data protection legislation.

To ensure the school network is used safely, this school:

- Ensures staff read and sign the Staff ICT Acceptable Use Policy and that they have read and understood the school's ICT & e-safety Policy. Staff personal network logon accounts provide controlled access to online services from school systems
- uses role based access permissions to the schools MIS system where higher level access requires two factor authentication
- Provides pupils with appropriate access to the school's systems and online within the terms agreed by the *Pupil ICT Acceptable Use Policy* for the Junior or Senior school
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use a teacher or another member of staff's account as these have wider access and inappropriate use could damage data, systems or inappropriately expose confidential data
- Has set-up the network with separate shared work areas for pupils and staff. Staff and pupils are shown how to save work and access work from these areas
- Requires all users to always log off when they have finished working or lock a computer when they temporarily leave a computer or device unattended
- Where a member of the school community finds a logged-on machine, we require them to always log-off the previous user and then log-on again as themselves
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or the computer has crashed
- Has set-up the network and systems to, wherever possible, block the download and running of unauthorised executable files, programs or apps
- Makes clear that staff are responsible for checking that any ICT equipment that may go home with them has appropriate encryption and / or security software maintained, such as anti-virus software
- Makes clear that staff are responsible for ensuring that any computer device loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs
- Maintains equipment to ensure Health and Safety is followed
- Ensures that access to the school's network resources from remote locations by staff is restricted and secure
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved secure mechanisms provided by the school Network Manager
- Makes clear the responsibilities for the daily backup of MIS and finance systems and other important files
- Has a disaster recovery system in place for critical data that includes a secure, remote backup of critical data
- Requires that in the event any pupil level data and confidential data needs sending over the Internet that it is encrypted or only available within an appropriately secure encrypted system
- Follows current technical advice on network security matters systems have been configured to prevent unauthorised access or malicious use of the school network and systems
- Our wireless network uses current industry standard security mechanisms and is deemed suitable for educational use
- All ICT equipment is properly installed, maintained and meets appropriate health and safety standards wherever applicable
- Ensures the ICT systems are reviewed with regard to security and emerging threats.

Passwords policy

- This school makes it clear that staff and pupils must always keep their passwords private, must not share them with others and must not leave them where others can find them. This is to ensure that individual members of the school community have access to services and data that are appropriate to their role and to maintain the confidentiality of personal data
- All staff and senior pupils have their own unique username and private passwords to access school systems
- We require all staff to use second factor authentication to access Google Workspace and the pupil management information system
- We require staff and pupils to choose strong passwords for their logon accounts

Email & communications

This school:

- Provides staff with a @knightsbridgeschool.com email account for their professional use which should always be kept separate from personal email
- Does not publish the email addresses of pupils or staff on the school website. We use anonymous or group email addresses
- Will contact the Police if one of our staff or pupils receives an email that we consider is particularly disturbing or we believe breaks the law
- Will ensure that current email accounts are maintained and up to date
- Knows that spam, phishing and virus attachments can make emails dangerous. We use layered technologies to help protect users and systems in the school but ask staff and pupils to remain vigilant when accessing unsolicited emails, especially those with click through links and/or attachments

Pupils:

- Pupils are introduced to and use email as part of the ICT classes
- Pupils must only use school email systems for school purposes
- Pupils are taught about the safety and 'netiquette' of using email both in school and at home, i.e. they are taught:
    - not to give out their email address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent / guardian
    - that an email is a form of publishing where the message should be clear, short and concise
    - that any email sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper
    - they must not reveal private details of themselves or others in email, such as address, telephone number, etc
    - to 'Stop and Think Before They Click' and never to open unsolicited attachments or click through links
    - that they should think carefully before sending any attachments
    - embedding adverts is not allowed;
    - that they must immediately tell a teacher or responsible adult if they receive an email which makes them feel uncomfortable, is offensive or bullying in nature

- never to respond to malicious or threatening messages
- not to delete malicious or threatening emails, but to keep them as evidence of bullying
- not to arrange to meet anyone they meet through email without having discussed with an adult and taking a responsible adult with them
- that forwarding 'chain' emails is not permitted

- Pupils sign the school ICT Acceptable Use Policy Agreement Form to say they have read and understood the e-safety rules, including email use and we explain how any inappropriate use will be dealt with

Staff:

- Should only use school email & communication systems for professional purposes
- Understand that access to personal email accounts may be blocked when in school
- Should never use email to transfer staff or pupil personal data unless sent by the authorised secured messaging service
- Must understand that email sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper. That it should follow the school guidelines:
  - the sending of multiple or large attachments should be limited; it may also be restricted by the provider of the service being used
  - the sending of chain letters is never permitted
  - embedding adverts is not allowed

- Must sign their agreement to the Staff ICT Acceptable Use Policy and have read and understood the e-safety rules and know how any inappropriate use will be dealt with.

Parent Portal (& KS Education Online when in use)

This school requires all users of the parent portal and KS Online to ensure:

- Spelling and grammar is checked before publishing pages content
- Links to external content are regularly checked by the author or owner of the content to ensure that they are working
- Content is regularly updated and old or irrelevant content is removed
- That any content that is reused from other sources or is subject to copyright is clearly shown and properly acknowledged
- That any forms and policies uploaded to the parent portal are checked to ensure they are the most up to date and approved versions of document and they are uploaded in a read only format (e.g. a PDF)
- Calendar entries are for group, class or whole school events and should not include individual meetings or private, in-school only events or meetings
- All calendar entries added or updated should be checked off against the school diary before publishing.

The Parent Portal is managed by the school administration staff.

- The school administration team are responsible for regularly monitoring and moderating the content of material posted to the Parent Portal

School website

- The Principal takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained
- Uploading of information is restricted to our designated website authors
- The school website complies with the statutory DfE guidelines for publications as is applicable to independent schools
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status
- The point of contact on the web site is the school address, telephone number and we use a general email contact address. Home information or individual email identities will never be published
- Photographs published on the website never show full names
- We will not use pupils' names when saving images in the file names or in the tags or meta data when publishing to the school website
- We will be vigilant and endeavour not to use embedded geo-data in respect of stored images

Social networking

This section should be read in conjunction with the school's Safeguarding Policy and the Staff Code of Conduct.

- Teachers are instructed not to run social network groups for pupil use on a personal basis or to 'friend' pupils in their own personal social networking accounts
- School staff will ensure that in private use:
    - No reference should be made in social media to pupils/pupils, parents/guardians or school staff
    - They do not engage in online discussion on personal matters relating to members of the school community
    - Personal opinions should never be attributed to the school and to refrain from publishing any personal opinions that could be interpreted as bringing the school into disrepute
    - The security settings on personal social media profiles are regularly checked to minimise risk of leakage or loss of personal information.

CCTV

Knightsbridge School has CCTV for site security and for pupil and staff safety. Access to recordings is restricted to members of the SLT, administration, IT and site management teams. Recordings are never shared without permission except where disclosed to the Police as part of a criminal investigation.

We reserve the right to use CCTV recording on occasions to share best practice and for training purposes.

5. Data Security & Protection: Management Information System Access and Data Transfer

Strategic and operational practices

At this school:

- Simon Harrison is the Data Protection Lead
- Staff are clear that the Data Protection Lead oversees all aspects of the Data Protection Policy and compliance and know to report any incidents where data protection may have been compromised
- All staff are DBS checked and records are held in one secure central location by the Bursar
- We ensure all pupils understand and sign agreement to the ICT Pupil Acceptable Use Policy (AUP)
- We ensure all parents understand and sign agreement to the Home-School Contract for the Safe use of The Internet and Digital Technologies
- We ensure all staff understand and sign this ICT end e-safety Policy
- We grant access to any other third party who has been granted access to school ICT systems, including directors of the school
- The ICT AUPs, Parent Home-School Internet Contract and Staff Handbook each make clear the responsibilities of users with regard to data security, passwords and access
- We follow Local Authority guidelines as they apply to the school for the transfer of any confidential data, such as MIS data or reports of children, to professionals working in the Local Authority or their partners in Children's Services/Family Services, Health, Welfare and Social Services
- We will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purpose it was collected for
- Data held must be accurate and up to date. Inaccuracies are corrected without unnecessary delay
- We have clear and understood arrangements for access, security, storage and transfer of personal data, including, where necessary, adequate contractual clauses or safeguards where personal data is passed to third parties e.g. cloud service providers or when taken off site
- The lawful basis for processing personal data (including, where relevant, consent) has been identified and documented and details provided in the relevant Privacy Notices
- Where special category data is processed, a lawful basis and a separate condition for processing have been identified
- Procedures must be in place to deal with the individual rights of the data subject i.e. a Subject Access Requests to see all or a part of their personal data held by the data controller
- We understand data retention policies and the routines for deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from an information risk incident which recognises the requirement to report relevant data breaches to the ICO within 72 hours of the breach, where feasible
- School staff with access to setting-up usernames and passwords for email and network access are working within the approved system and follow the security processes required by those systems
- All staff receive data protection training as part of their INSET programme
- We ask staff to undertake at least annual housekeeping to review, remove and destroy any digital materials and documents which need no longer be stored.

Technical solutions

- Staff have secure area(s) on the network and in the cloud to store their own work related files
- Computers can be set to lock screen when left inactive for a period of time
- Staff are required to encrypt any sensitive information if it must be taken off site
- The Schools MIS system role based permissions and all access requires two factor authentication.
- We use strong encryption and user authentication for remote access into our systems

- We store confidential printed material in lockable storage cabinets in a locked office
- All servers are in a lockable server room and managed by DBS checked personnel.
- We use a remote, secure backup facility. Backup data is encrypted in transit
- We comply with the WEEE directive on equipment disposal by using an approved or recommended disposal company for disposal of equipment where any protected or restricted data has been held
- Paper based sensitive information is shredded, using cross cut shredder or collected by secure data disposal service.

6. Equipment and Digital Content

Pupil Chromebooks & devices

- All senior pupils are issued with Chromebooks to support teaching and learning at school; junior pupils have access to shared Chromebooks
- Senior pupils will make every effort to look after their assigned Chromebooks and report any issue or damage to their teacher straight away
- Senior pupils will ensure they use only their assigned Chromebook and not another pupils Chromebook
- Chromebooks will be returned and plugged in to their designated classroom secure charging cabinet at the end of each day.
- Junior class teachers and senior house tutors are responsible for checking all Chromebooks are plugged in and securing the cabinets at the end of each day

Teacher iPads & Chromebooks

- All teachers are assigned devices to support their school work and must sign and agree to the term of use for the device
- Teachers are responsible for the security of their assigned device, charger, charger cable, protective case or other peripheral and must return all items on leaving employment or on long term leave from the school
- Any damage or loss of a school device (or peripheral) must be reported the the IT team immediately so that appropriate action can be taken to repair or retrieve it

Pupils' use of personal devices

- The School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety when travelling to and from school – in this case authorisation will be given
- Pupil mobile phones or communications devices which are brought into school must be left at school reception immediately on arrival to school, turned off or engaged in 'flight mode' and collected again when leaving at the end of the day
- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in school reception. Mobile phones and devices will be released to parents or guardians in accordance with the school policy

- Phones and devices must never be taken into examinations (including ISEB). Pupils found in possession of a mobile phone during such examinations may be reported to the appropriate examining body and/or senior school. This may result in the pupil's withdrawal from either that examination or all examinations
- If a pupil needs to contact his or her parents or guardians, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school reception office
- Pupils should protect their phone numbers by only giving them to trusted friends and family members Pupils will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of the risks and their consequences
- Pupils may be provided with school mobile devices to use in specific learning activities but only under the supervision of a teacher or other member of staff.

Use of personal devices to support access to learning

There may be occasional circumstances where we will allow the use of specific personally-owned devices in order to support learning or the access to learning. For example, allowing the use of Kindle book readers to support pupils reading under the supervision of the Learning Support department. In all such circumstances the use of personally owned devices at school must have the explicit permission of a member of the SMT or SLT.

As with any other personal device brought to school, the responsibility for the safety of the device rests with the owner and the school will accept no liability for any loss or damage to these devices.

Staff use of personal devices (BYOD Policy)

- Personal mobile phones and devices brought into school are done so entirely at the owner's risk. The School accepts no responsibility for the loss, theft, damage or wear and tear of any personal device brought into or used at school
- Staff mobile phones or communications devices must be switched off or kept on silent and out of sight of pupils at all times, except when necessary to conduct their duties off-site or in the event of an emergency
- Mobile phones and personally-owned communication devices should not be used during lessons or formal school time. They should be switched off or on silent at all times, and should never be used for personal reasons
- No images or videos should be taken on personally-owned mobile devices without the prior consent of the person(s) concerned and in the case of pupils, without the consent of a teacher or supervising member of staff; any images taken in school must be downloaded from the device and deleted from the device before the end of the day
- Whenever possible staff must use school provided ICT facilities for making contact with parents, guardians or pupils when outside of school. In limited circumstances, such as school visits and trips, staff may have to use personal mobile phones for school business but only within the bounds of their professional capacity
- In the event of the above, staff should hide their own mobile number (by either configuring their caller visibility or first inputting 141) for confidentiality purposes

- The Bluetooth or similar peer connectivity functionality of mobile phones or communications devices should be 'hidden' or switched off at all times and not be used to send images, files or messages to others mobile phones or to connect with other devices
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity then it will only take place when approved by a member of the senior leadership team
- Staff are responsible for the security of their own devices and must ensure that security updates are applied regularly where applicable, including individual app updates
- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence, bullying or radicalisation. Staff personal mobile devices may be searched in the event the Head or Designated Safeguarding Lead suspects that it may contain inappropriate material
- All use of mobile phones and personal devices while in school, during school hours or on school business is to be open to scrutiny and the Head can withdraw or restrict authorisation for use of mobile phones or devices at any time if it is to be deemed necessary

If a member of staff breaches the school policy then disciplinary action may be taken.

Apps and device management

- The use of personally owned apps or services to support teaching and learning are allowed at the discretion of the Head but the school is not responsible for the cost of purchasing or maintaining any such app or service
- Under no circumstances is confidential data of other members of the school community to be used or stored within personal apps or services
- Apps and services authorised, purchased, and/or managed through the school's official accounts are the property of the school and will be distributed to accounts on devices that are managed by the school. In some limited circumstances they may be distributed for use on a personally owned device, but will be only done so for purposes that fall within the user's professional capacity at school.

Digital images and video

In this school:

- We gain parental / guardian permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school
- We do not identify pupils in online photographic or video materials or include the full names of pupils in the credits of any published school produced video materials
- Staff sign the school's ICT Acceptable Use Policy for Staff and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils
- If specific individual pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for their long term use

- The school blocks pupil access to popular social networking and image sharing sites unless there is a specific approved educational purpose
- Pupils are taught about how images can be manipulated in their e-safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space when out of school. They are taught to understand the need to maintain privacy settings so as not to make public any personal information
- Pupils are taught that they should never post images or videos of others without their permission. We teach them about the risks associated with providing information with images that can reveal the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or peer-on-peer abuse.

Asset disposal

- Details of all school-owned hardware will be recorded in a hardware inventory
- Details of all school-owned software will be recorded in a software inventory
- All redundant equipment will be disposed of through appropriate channels. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data
- All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007

Reviewed by: Simon Harrison (IT Consultant) & Gill Conlon (DSL)	**Date:** Sep 2022
Approved by: **Signed**: Shona Colaço (Head)	**Date**: Sept 2022
This policy will be reviewed annually.	