Acceptable Use Policy

Kingsway Primary School

Governor Committee Responsible:	FGB	**Staff Lead**:	Steve Flower
Status	Non-statutory	**Review Cycle**	Annual
Last Review	13th October 2025	**Next Review Date**	September 2026

Contents

1. Introduction and aims 2
2. Relevant legislation and guidance 2
3. Definitions 2
4. Unacceptable use 3
5. Staff (including governors, volunteers, and contractors) 4
    5.1. Access to school ICT facilities and materials 4
        5.1.1 Use of phones and email 4
        5.1.2 Recording phone calls 5
        5.1.3 Use of personal mobile phones for staff 5
        5.1.4 Use of Class Dojo 6
5.2 Personal Use 6
        5.2.1 - Personal social media accounts 6
5.3 - School Social media accounts 7
5.4 - Remote Access 7
5.5 - Photography 7
5.6 - Monitoring of school network and use of ICT facilities 7
6. Pupils 8
    6.1 - Access to ICT facilities 8
    6.2 - Search and deletion 9
    6.3 - Unacceptable use of ICT and the internet outside of school 9
7. Parents/carers ..... **Error! Bookmark not defined.**10
8. Data security ..... **Error! Bookmark not defined.**11
9. Internat Access; Protection from cyber attacks ..... **Error! Bookmark not defined.**12
10. Online Safety: Misinformation, and Emerging Technology Risks 13
11. Monitoring and review ..... **Error! Bookmark not defined.**15
12. Related policies ..... **Error! Bookmark not defined.**15
- Breaches of Policy 16
    Appendix 1: Scoial media guidance for staff ..... **Error! Bookmark not defined.**17
    Appendix 2: Acceptable use agreement for younger pupils 20
    Appendix 3: Acceptable use agreement for older pupils 21
    Appendix 4: Acceptable use agreement for staff, governors, volunteers and visitors. **Error! Bookmark not defined.**22
    Appendix 5: Glossary of cyber security terminology 23
    Appendix 6: Class Dojo Agreement Form 25

1. Introduction and aims

ICT is an integral part of the way our school works, and is a critical resource for pupils, staff, governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the school. However, the ICT resources and facilities our school uses also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policy on data protection, online safety and safeguarding
- Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching pupils safe and effective internet and ICT use

This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors. Breaches of this policy may be dealt with under our Staff Conduct policies and processes.

2. Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- Education and Inspections Act 2006
- Keeping Children Safe in Education 2024
- Searching, screening and confiscation: advice for schools 2022
- National Cyber Security Centre (NCSC): Cyber Security for Schools
- Education and Training (Welfare of Children) Act 2021
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Meeting digital and technology standards in schools and colleges

3. Definitions

- **"ICT facilities":** includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service

- **"Users":** anyone authorised by the school to use the ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors
- **"Personal use":** any use or activity not directly related to the users' employment, study or purpose
- **"Authorised personnel":** employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities
- **"Materials":** files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites, and blogs

4. Unacceptable use

The following is considered unacceptable use of the school's ICT facilities by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, staff, or other members of the school community
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the school's ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to the school's ICT facilities
- Removing, deleting or disposing of the school's ICT equipment, systems, programmes or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, misogynistic, extremist, racist, antisemitic or discriminatory in any other way

- Using AI tools and generative chatbots (such as ChatGPT and Google Bard):
    - During assessments, including internal and external assessments, and coursework
    - To write their homework or class assignments, where AI-generated text or imagery is presented as their own work
- Using AI tools to generate inappropriate imagery.

This is not an exhaustive list. The school reserves the right to amend this list at any time. The headteacher will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

4.1 Exceptions from unacceptable use

Where the use of school ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the headteacher's discretion.

- Using AI to:
    - As a research tool to help them find out about new topics and ideas
    - When specifically studying and discussing AI in schoolwork, for example in IT lessons or art homework about AI-generated images. All AI-generated content must be properly attributed

4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's policies on behaviour policy and staff conduct and disciplinary.

5. Staff (including governors, volunteers, and contractors)

5.1 Access to school ICT facilities and materials

The school's business manager manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the school's ICT facilities.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the school business manager.

Supply teachers and temporary staff will use the Supply Teacher login which can be obtained from the office. Staff must not let supply teachers use their own unique log in.

5.1.1 Use of phones and email

The school provides each member of staff with an email address.

This email account should be used for work purposes only.

All work-related business should be conducted using the email address the school has provided.

Staff must not share their personal email addresses with parents and pupils, and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error which contains the personal information of another person, they must inform the business manager immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parents or pupils; this also includes past pupils under the age of 18. Staff may use their own phones to contact other staff members when on school trips but should use a school-provided phone when contacting parents or other professionals. In case of emergency, where they need to use their own phone, they should withhold their number by first dialling 141.

School phones must not be used for personal matters.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4.

Emails sent from school should contain the same professional levels of language and content as applied to letters or other media. Staff are responsible for the emails sent, even if forwarded from another source, and for any contacts you make that might result in inappropriate emails being received.

Posting anonymous messages and forwarding chain letters is forbidden.

5.1.2 - Recording phone calls

The school may record incoming and outgoing phone conversations.

If calls are recorded, callers must be made aware that the conversation is being recorded and the reason for doing so. Where calls are automatically recorded, reasons will be explained. For instance:

- "All calls to the school office are recorded to aid administrators."
- "Calls are recorded for use in staff training."

Where staff require specific phones conversations to be recorded, they should speak with the headteacher to seek approval. To this aim, all non-standard recordings of phone conversations must be pre-approved and consent obtained from all parties involved. Such conversation may (not exclusively) relate to:

- Discussing a complaint raised by parent/carers or a member of the public
- Calling parents/carers to discuss behaviour or sanctions.
- Taking advice from relevant professionals regarding safeguarding, special educational needs (SEND) assessments, etc.

5.1.3. - Use of Personal Mobile Phones for Staff:

Personal mobile phones should not generally be needed or used by staff, except as set out in the guidelines below:

- Should staff need to use their mobile phone on school site, best practice is that mobile phones, wherever possible, should not be used in the presence of the children. In EYFS, personal mobile phones should never be used in the presence of children.
- Staff should ensure that any personal mobile device brought on site are stored in a secure location (a bag or drawer) and are not accessible while working with children.

- Mobile phones should not be used during lesson times either to make or receive calls, unless there is an emergency.
- Staff should exercise caution when giving their mobile number to parents as this could be misconstrued. We are aware that some staff members are also parents at the school and this is an exception to this rule.
- Trips and Visits Offsite: staff may use their mobile phones when responsible for children away from school, only in an emergency. Typically, however, the staff member in charge should take one of the school mobile phones when off site. This phone should be used when communicating with parents. Other staff members on the trip or offsite should carry their mobile phones so they can communicate with colleagues when necessary or in an emergency.
- No photographs, videos or images of children should be captured using a personal mobile phone; only school devices should be used
- Staff are not permitted to connect any personal device to any part of the school ICT facilities without the permission of the Headteacher or School Business Manager. This includes connecting mobile phones, even for charging, to school laptops.
- All personal data in relation to the school must not be stored on personal mobile devices.

5.1.4 – Use of Class Dojo

As a school we use Class Dojo to share messages with parents. All staff must ensure that posts and messages on Class Dojo are written in a professional manner and given the same consideration as any other communication with parents.

When parents contact staff via class Dojo, teachers should not be expected to respond outside of normal working hours, however they may choose to do so to best suit their working patterns and facilitate a reasonable response frame.

5.2 Personal use

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The school business manager may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during contact time
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the school's ICT facilities to store personal non-work-related information or materials (such as music, videos, or photos).

Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities (see section 5.6). Where breaches of this policy are found, disciplinary action may be taken.

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the school's safeguarding policy – section 10.

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance putting personal details in the public domain, where pupils and parents could see them.

Staff should take care to follow the school's guidelines on social media (see appendix 1) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.2.1 Personal social media accounts

Members of staff should ensure that their use of social media, either for work or personal purposes, is appropriate at all times.

The school has guidelines for staff on appropriate security settings for social media accounts (see appendix 1).

5.3 Remote access

We allow staff to access the school's ICT facilities and materials remotely.

All staff laptops are set up for remote access to the school server on home networks. This is managed by the School Business Manager and ICT support technician.

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and take such precautions as the business manager may require from time to time against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

Where staff engage in remote learning with children, they must comply with all safety measures outlined in our Remote Learning Policy.

5.4 School social media accounts

The school has official social media platforms (Facebook and Instagram) which are managed by the website manager. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

SOKs also has a private Facebook page which is managed by the SOKs chair. This is a private group only for parents of children at Kingsway and membership is monitored through security questions.

The school has guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times.

If any staff member is targeted by a member of the community online, they should not respond but capture the comments and refer this to the DSL for further guidance and support. The DSL will seek legal and Police support as necessary.

Further information may be sought here:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf

5.5. Photography

Staff **must** only use school equipment to record, or take photographs of pupils, and only then if the relevant permission has been obtained. Photos must only be stored using school equipment and must not be uploaded to any home devices.

5.6 Monitoring of school network and use of ICT facilities

The school reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage

- Email accounts including e-mail and their contents
- Telephone calls
- User activity/access logs
- Any other electronic communications
- Files and folders stored on the network

The Headteacher or School Business Manager will inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The school monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

Our governing board is responsible for making sure that:

- The school meets the DfE's filtering and monitoring standards
- Appropriate filtering and monitoring systems are in place
- Staff are aware of those systems and trained in their related roles and responsibilities
    - For the leadership team and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns
- It regularly reviews the effectiveness of the school's monitoring and filtering systems

The school's designated safeguarding lead (DSL) will take lead responsibility for understanding the filtering and monitoring systems and processes in place.

Where appropriate, staff may raise concerns about monitored activity with the school's DSL and ICT manager, as appropriate.

6. Pupils

6.1 Access to ICT facilities

Children have access to the following ICT facilities:

- Laptop computers which are used both in the library and in classrooms.
- Tablets for use in class.
- Chromebooks for use in all classrooms

All ICT facilities should only be used in the presence of staff who should always monitor children's use – this includes the use of any software (including AI enabled platforms) accessed through the hardware systems provided for learning.

6.2 Search and deletion

Under the Education Act 2011, the headteacher, and any member of staff authorised to do so by the headteacher, can search pupils and confiscate their mobile phones, computers or other devices that the authorised staff member has reasonable grounds for suspecting:

- Poses a risk to staff or pupils, **and/or**
- Is identified in the school rules as a banned item for which a search can be carried out **and/or**
- Is evidence in relation to an offence

This includes, but is not limited to:

- Pornography
- Abusive messages, images or videos
- Indecent images of children
- Evidence of suspected criminal behaviour (such as threats of violence or assault)

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher / DSL
- Explain to the pupil why they are being searched, and how and where the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation (if the pupil refuses to co-operate, the school will proceed in line with the current behaviour policy.
- The authorised staff member should:
- Inform the DSL (or deputy) of any searching incidents where they had reasonable grounds to suspect a pupil was in possession of a banned item(s).
- Involve the DSL (or deputy) without delay if they believe that a search has revealed a safeguarding risk

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on a device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on a device, the staff member should only do so if they reasonably suspect that the data has been, or could be, used to:

- Cause harm, **and/or**
- Undermine the safe environment of the school or disrupt teaching, **and/or**
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / headteacher / member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider whether the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as is reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, **and/or**
- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image

- **Not** copy, print, share, store or save the image
- Confiscate the device and report the incident to the DSL (or deputy) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on searching, screening and confiscation and the UK Council for Internet Safety (UKCIS) et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy / searches and confiscation policy – guided by the updated DfE guidance, which came into force on 1st September 2022

Any complaints about searching for, or deleting, inappropriate images or files on pupils' devices will be dealt with through the school complaints procedure.

6.3 Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with the behaviour policy and/or the anti-bullying policy, if a pupil engages in any of the following **at any time** (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other pupils, or other members of the school community
- Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language

7. Parents / Carers

7.1 Access to ICT facilities and materials

Parents do not have access to the school's ICT facilities as a matter of course.

However, parents working for, or with, the school in an official capacity (for instance, as a volunteer or as a member of SOKs) may be granted an appropriate level of access, or be permitted to use the school's facilities at the headteacher's discretion.

Where parents are granted access in this way, they must abide by this policy as it applies to staff.

7.2 Communicating with or about the school online

We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

8. Data security

The school takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee security. Staff, pupils, parents and others who use the school's ICT facilities should use safe computing practices at all times.

8.1 Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or pupils who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.

8.2 Software updates, firewalls, and anti-virus software

All of the school's ICT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

Any personal devices using the school's network or being used to conduct school business must all be configured in this way.

8.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy.

8.4 Access to facilities and materials

All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices.

These access rights are managed by the School Business Manager

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the school business manager immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

When users need to leave the room whilst their computer is logged on, the screen should be locked.

8.5 Encryption

The school ensures that its devices and systems have an appropriate level of encryption.

School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the headteacher.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the ICT manager/SBM.

9. Internet access

The school wireless internet connection is secured and staff and children have access to different drives on the server.

Unfortunately, along with a wealth of useful educational sites on the internet, there are also sites which contain inappropriate materials which it would be unacceptable for children to gain access to.

To ensure that children access the internet within a safe environment our internet service is filtered by the SWGfL. This excludes unacceptable material through filtering lists of inappropriate sites to which access is barred when using the school's line. This will include AI platforms recognised to present such risks, as well as those sites known to share misinformation/disinformation (see Section However, there is a very small risk that inappropriate material may occasionally get through unfiltered. If this happens the SWgFL should be contacted and the headteacher should be informed.

To further improve safety, the HT/DSL regularly monitors the effectiveness of filtering systems and works in partnership with the IT Provider to improve safety.

9.1.0 Protection from cyber attacks

The school will:

- Work with governors to make sure cyber security is given the time and resources it needs to make the school secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security (SchoolPro TLC provider)
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether our IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Put controls in place that are:
    - **Proportionate**: the school will verify this using a third-party audit to objectively test that what it has in place is effective
    - **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe
    - **Up to date:** with a system in place to monitor when the school needs to update its software
    - **Regularly reviewed and tested**: to make sure the systems are as effective and secure as they can be
- Back up critical data is completed on a daily basis, automatically and to a cloud-based system (Veeam) which is not connected to the school network. In addition, Business Managers and the HT will outline a disaster recovery plan, to action, in the event of a cyber-attack on any school system – preventing or limiting impacts of any malicious actions from internal or external sources: this should include how this is communicated to all parties effected by any breach.
- Delegate specific responsibility for maintaining the security of our management information system to our IT providers, which are a combination of Gloucestershire County Council and the IT Manager at Rednock Secondary School.

- Make sure staff:
    - Dial into our network using a virtual private network (VPN) when working from home
    - Enable multi-factor authentication where they can, on things like school email accounts
    - Store passwords securely using a password manager
- Have a firewall in place that is switched on

9.1 Pupils

Internet access is a necessary part of planned lessons. It is an entitlement for pupils based on responsible use. Teachers will ensure that:

- Pupils will be taught how to use a range of age-appropriate online tools in a safe and effective way.

- For Foundation and Key Stage 1, access to the Internet will be by teacher or adult demonstration or suitable skills will be taught / activities provided to ensure that children are only accessing appropriate sites.

- For Years 3 and 4, access to the Internet will be by teacher or adult demonstration. Pupils will access teacher-prepared materials or specific sites deemed safe by staff and searching will only take place using the search engine 'Swiggle.'

- For Years 5 and 6, Internet access will be granted to a whole class as part of the scheme of work, after a suitable introduction to the rules for responsible Internet use. In the normal event, access will be guided by using sites listed in the school Intranet pages and safe search techniques will be taught.

Our Acceptable Use policy is covered with pupils within our computing curriculum regularly and children are taught about safe and responsible use repeatedly.

9.2 Parents and visitors

Parents and visitors to the school will not be permitted to use the school's Wi-Fi unless specific authorisation is granted by the headteacher.

The headteacher will only grant authorisation if:

- Parents are working with the school in an official capacity (e.g. as a volunteer or as a member of SOKs)
- Visitors need to access the school's Wi-Fi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

Staff must not give the Wi-Fi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

10. Online Safety: Misinformation, and Emerging Technology Risks

10.1 Overview

This section sets out expectations for safe, responsible, and respectful use of digital technologies, including artificial intelligence (AI) tools, social media, and online communication platforms. It reflects the latest *Keeping Children Safe in Education (KCSIE)* guidance and recognises the importance of safeguarding learners from online risks such as misinformation, disinformation, cyberbullying, grooming, and misuse of AI systems.

10.2 Misinformation and Disinformation

- Users must critically evaluate online content and verify information before sharing it.
- The creation or sharing of false or misleading information (misinformation or disinformation), including through social media, messaging apps, or AI tools, is strictly prohibited.

- Staff and pupils should report suspected misinformation or harmful online content to the Designated Safeguarding Lead (DSL) or Online Safety Lead.
- The school will support digital literacy education to help pupils identify trustworthy sources and understand bias, manipulation, and online influence

10.3 Cyberbullying and Online Harassment, Inc. use of AI (see section 9, also)

- Any form of bullying, harassment, or intimidation conducted through digital means — including messages, posts, comments, or AI-generated content — is unacceptable.
- Users must not use technology to cause harm, distress, or humiliation to others.
- Incidents of cyberbullying will be treated as safeguarding concerns and may result in disciplinary action.
- The school promotes a culture of respect and kindness online and offline, supporting pupils in understanding the impact of their digital behaviour.

10.4 Online Grooming and Exploitation

- Users must not engage in or facilitate any form of online grooming, sexualised communication, or exploitation.
- Any approach from an unknown person seeking personal information, private images, or inappropriate contact must be reported immediately to a trusted adult or the DSL.
- Staff will receive training to identify and respond to signs of online grooming, radicalisation, and coercive behaviour.
- Pupils will be taught about healthy relationships, consent, and how to recognise and report unsafe online contact

10.5 Artificial Intelligence (AI) and Emerging Technologies

- AI tools must be used ethically, responsibly, and in line with educational objectives.
- Users must not use AI systems to:
    - Generate or spread false or harmful information;
    - Create, manipulate, or distribute inappropriate, sexualised, or discriminatory content;
    - Impersonate others or produce misleading outputs;
    - Circumvent academic honesty or plagiarism expectations.
- Staff must ensure pupils understand the limitations, biases, and potential risks of AI tools.
- AI systems used within the school must be vetted for safety, privacy, and compliance with data protection and safeguarding standards.

10.6 Digital Citizenship and Education

- The school will deliver an ongoing digital citizenship curriculum that develops pupils' understanding of online safety, respect, and critical thinking.
- Pupils will learn how to manage their digital footprint, protect their privacy, and use technology positively.
- The school encourages collaboration between pupils, staff, and parents to foster a safe and supportive digital community.

10.7 Staff Conduct Online

- Staff are expected to model positive online behaviour and adhere to the same standards of respect and integrity expected offline.

- Staff must not engage in, support, or condone misinformation, cyberbullying, or the misuse of AI.
- Professional boundaries must be maintained at all times, including through the responsible use of communication tools and social media.

10.8 Data Protection and Privacy

- Users must respect data protection laws and confidentiality requirements when using digital technologies.
- Personal information must only be shared for legitimate educational purposes and through secure systems.
- AI and online platforms that collect or process data must be assessed for compliance with data protection and safeguarding expectations before use.

10.9 Reporting and Support

- Any concerns relating to online harm, misinformation, grooming, cyberbullying, or inappropriate use of AI should be reported to the DSL or Online Safety Lead.
- The school will respond promptly and proportionately to incidents, following safeguarding and disciplinary procedures as appropriate.
- Support will be offered to any pupil affected by online harm, including access to pastoral care and external support services.

10.10 Monitoring and Review

- This section of the Acceptable Use Policy will be reviewed annually in line with updated KCSIE guidance and technological developments.
- Feedback from pupils, staff, and parents will inform updates to ensure the policy remains relevant and effective in addressing emerging online risks.

11. Monitoring and review

The headteacher/DSL and the SBM/IT provider monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every year.

The governing board is responsible for approving this policy.

12. Related policies

This policy should be read alongside the school's policies on:

- Online safety
- Safeguarding and child protection
- Behaviour
- Staff Code of Conduct
- GDPR
- Anti-bullying.
- RSE

BREACHES OF THE POLICY

- Any breach of this policy may be investigated and may lead to disciplinary action being taken against the staff member/s involved in line with School Disciplinary Policy and Procedure.

- A breach of this policy leading to breaches of confidentiality, or defamation or damage to the reputation of the school or any illegal acts or acts that render the school or the County Council liable to third parties may result in disciplinary action or dismissal.

- Contracted providers of the school must inform the relevant service or County Council officer immediately of any breaches of this policy so that appropriate action can be taken to protect confidential information and limit the damage to the reputation of the service and the County Council. Any action against breaches should be according to contractors' internal disciplinary procedures.

If you are in doubt about any of the above, please seek advice.

Appendix 1: Social Media guidelines for staff:

Social Media

Social Media is used increasingly across society and is recognised as a hugely valuable communication tool. However, the open nature of the internet means that social networking sites can leave professionals (such as teachers and other staff working in education) vulnerable if they fail to observe a few simple precautions. This policy is designed to protect school staff and pupils from potential harm or from becoming victims of radicalisation, extremism and malicious, upsetting or inadvisable contact. (For detailed explanations please see the School Safeguarding Policy)

- Staff members **must not** identify themselves as employees of the school in their personal webspace apart from professional websites such as LinkedIn. This is to prevent information on these sites from being linked with the school and the County Council and to safeguard the privacy of staff members, particularly those involved in providing sensitive frontline services.

- Staff members **must not make contact through any personal ICT or social medium with any pupil**, whether from our school or any other school, unless the pupil* is your own family member OR an existing close family friend. School does not expect staff members to discontinue contact with their own family members or significant family friends via personal social media, however care should be taken not to communicate with friends of the family member who may be school pupils.

- We strongly advise against accepting social media 'friend' invites from parents of pupils. There may exceptions to this e.g. the parent is a family member.

- If staff members need to communicate with parents or pupils for work purposes they can only do so through the official school email, Class Dojo or school phone. Personal email addresses/phone numbers **must not** be shared with pupils or parents.

- Staff members **must decline 'friend requests' from pupils or former pupils (those who have left the school within the last 5 years)** they may receive in their personal social media accounts. Pupils/parents will be informed that this will be the case on induction.

- On leaving school employment, staff members **must not** contact pupils by means of personal social media sites. Similarly, staff members must not contact pupils from their former schools by means of personal social media.

- Any information staff members have access to as part of their employment, including personal information about pupils and their family members, colleagues, County Council staff and other parties and service or County Council corporate information must not be discussed on their personal webspace or social media sites.

- Photographs, videos or any other types of image of pupils and their families or images depicting staff members who can be identified as school staff must not be published on personal webspace or social media sites.

- School or County Council email addresses and other official contact details must not be used for setting up personal social media accounts or to communicate through such media.

- Staff members must not edit open access online encyclopaedias such as *Wikipedia* in a personal capacity at work. This is because the source of the correction will be recorded as the employer's IP address and the intervention will, therefore, appear as if it comes from the employer itself.

- School logos or brands must not be used or published on personal webspace/social media sites (apart from professional websites such as LinkedIn)

- School does not permit personal use of social media or the internet during core contracted work hours. Access to social media sites for personal reasons is not allowed between 9am and 4.15pm (apart from during lunch breaks). Staff members are expected to devote their contracted hours of work to their professional duties.

- **Caution** is advised when inviting work colleagues to be 'friends' on personal social networking sites. Social networking sites blur the line between work and personal lives and it may be difficult to maintain professional relationships or it might be just too embarrassing if too much personal information is known in the work place. Staff **must not** use social media and the internet in any way to attack, insult, abuse or defame pupils, their family members, colleagues, other professionals, other organisations, School or the County Council.

    - Staff members **are advised to set the privacy levels of their personal social media sites as strictly as they can** and to opt out of public listings on social networking sites to protect their own privacy. Staff members should keep their passwords confidential, change them often and be careful about what is posted online; it is not safe to reveal home addresses, telephone numbers and other personal information. It is a good idea to use a separate email address just for social networking so that any other contact details are not given away. *(Please see the "Social networking – Guidelines for NASUWT members which sets out minimum recommended privacy settings for Facebook)*

What to do if…

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the headteacher about what's happening

A parent adds you on social media

- It is at your discretion whether to respond. Bear in mind that:

    Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school

    Pupils may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in

- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents

- If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Our Acceptable Use policy is covered with pupils within our computing curriculum regularly.

Appendix 2: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
In reception, I will learn to: • Only use a computer or touchscreen when my teacher says so • Use gentle hands with all computers and equipment • Only use the games and websites set up by my teacher • Tell my teacher if something goes wrong **In addition to this, in years 1 and 2 I will learn to:** • Log on and log off the school system safely • Open apps and websites only that my teacher has said I can use • Tell my teacher immediately if: ○ I click on a website by mistake ○ I find anything that I don't like • Use school computers for school work only • Tell an adult if I find something that is not working • If I am given a username and password, keep it to myself • Save my work on the school network • Check before I print anything **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these. I agree to supporting the school in keeping my child safe when working online by enforcing the expectations outlined in school policies.	
Signed (parent/carer):	**Date:**

Appendix 3: KS2, acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy **When I use the school's ICT systems (like computers) and get onto the internet in school I will:** • Always use the school's ICT systems and the internet responsibly and for educational purposes only • Only use them when a teacher is present, or with a teacher's permission • Keep my username and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or trusted adult) immediately if I find any material which might upset, distress or harm me or others including information or messages sent to me by other children • Always log off or shut down a computer when I'm finished working on it **I will not:** • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Log in to the school's network using someone else's details • Arrange to meet up with anyone I have met online without first consulting my parent/carer, or without adult supervision **If I bring a personal mobile phone or other personal electronic device into school:** • I will not use it on the school site at any time: during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission • I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online • I will hand my mobile phone in to the teacher as soon as I arrive **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these. I agree to supporting the school in keeping my child safe when working online by enforcing the expectations outlined in school policies.	
Signed (parent/carer):	**Date:**

Appendix 4: acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access, inappropriate material, including but not limited to material of a phobic, violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 5: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber-attack and the measures the school will put in place. They're from the National Cyber Security Centre (NCSC) glossary.

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
AI	The development of computer systems that can perform tasks that normally require human intelligence, such as learning, problem-solving, and decision-making.
Breach	When your data, systems or networks are accessed or changed in a non-authorised way.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Disinformation	False information that is deliberately created and shared to mislead or manipulate others.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Emerging Technologies	New and rapidly developing technologies — such as AI, robotics, virtual reality, and biotechnology — that have the potential to significantly change how we live, work, and learn.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.

TERM	DEFINITION
Misinformation	False or inaccurate information that is shared without the intent to deceive — often spread because people believe it is true.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Pharming	An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website address.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programmes designed to self-replicate and infect legitimate software programs or systems.
Virtual private network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly- targeted phishing attacks (where emails are made to look legitimate) aimed at senior people in an organisation.

Appendix 6

Kingsway Primary School
Valley Gardens, Kingsway
Gloucester, GL2 2AR

Telephone: 01452 881800
www.kingswayprimary.org.uk
admin@kingsway.gloucs.sch.uk

Kindness • Perseverance • Success

PARENTAL AGREEMENT FORM: Class Dojo

At Kingsway Primary School, we highly value parents' involvement in their child's education. To support this involvement, we use the Class Dojo App to Share information with you about your child's online journey. The App is available to download on a phone or tablet or through a web browser. All of this information is stored on a highly secure server which is monitored closely in line with GDPR regulations.

In order for us to be able to activate your child's accounts for Class Dojo, we need you to sign an agreement regarding how this is used.

Agreed guidelines for accessing and using your child's Class Dojo accounts:

As a parent I will…

- **Not** publish any of my child's observations, photographs or videos on any social media site, this applies even when observations only have your child in.
- Keep the login details within my trusted family.
- Speak to a member of staff if I experience any difficulties accessing my child's learning journey.
- Raise any concerns privately with the class teacher or other members of staff and not use a public forum.

I agree to the following guidelines:

Name of Parent/Carer (BLOCK CAPITALS) _____

Name of child: _____

Parent/Carer signature: _____ Date: _____

Preferred email address: _____