Kingsmead School & Sixth Form

ICT and Internet Acceptable Use Policy

This plan is reviewed annually in the autumn term.

Next Review Due: Nov 2026

History of Document:

Issue No.	Date Issued	Prepared By	Approved By	Comments
Issue 1	Nov 2023	D Finney	TB Nov 2023	Reformatted to new policy format
	Nov 2024	L Baker	TB Dec 2024	No changes
	Nov 2025	D Finney	TB Dec 2025	AI Updates, DUAA

Contents

1. Introduction and aims 3
2. Relevant legislation and guidance 3
3. Definitions 4
4. Unacceptable use 4
5. Staff (including trustees, volunteers, and contractors) 6
6. Pupils 9
7. Parents/carers 12
8. Data security 12
9. Protection from cyber attacks 14
10. Internet access 15
11. Monitoring and review 16
12. Related policies 16
Appendix 1: Facebook cheat sheet for staff 17
Appendix 2: Acceptable use of the internet: agreement for parents and carers 19
Appendix 3: Acceptable use agreement for older pupils 20
Appendix 4: Acceptable use agreement for younger pupils 21
Appendix 5: Acceptable use agreement for staff, trustees, volunteers and visitors 22
Appendix 6: Glossary of cyber security terminology 23

1. Introduction and aims

Information and communications technology (ICT) is an integral part of the way our school works, and is a critical resource for pupils, staff (including the senior leadership team), trustees, volunteers, and visitors. It supports teaching and learning, and the pastoral and administrative functions of the school.

However, the ICT resources and facilities our school uses could 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/carers, and trustees.
- Establish clear expectations for the way all members of the school community engage with each other online.
- Support the school's policies on data protection, online safety, and safeguarding.
- Prevent disruption that could occur 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 trustees, staff, pupils, volunteers, contractors, and visitors.

Breaches of this policy may be dealt with under our disciplinary procedure.

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
- Data (Use and Access) Act 2025 – The Information Commissioner's office is in the process of updating their published guidance with regards to the Data (Use and Access) Act 2025 (DUAA) which will come into effect in stages from June 2025 to June 2026. This policy will be updated if necessary as guidance is published.
- 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 2022
- 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:** 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 that may become available in the future which is provided as part of the school's ICT service.
- **Users:** anyone authorised by the school to use the school's ICT facilities, including trustees, staff, pupils, volunteers, contractors, and visitors
- **Personal use:** any use or activity not directly related to the users' employment, study or purpose agreed by an authorised user.
- **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 school's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs.

See appendix 6 for a glossary of cyber security terminology.

4. Unacceptable use

The following is considered unacceptable use of the school's ICT facilities. 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, 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, 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.
    - Where staff or student personal data is uploaded to an AI service where we do not have a data processing agreement or Data Protection Impact Assessment in place, this would be a breach of this policy, our data protection policy and UK legislation.
    - Where copyright material is uploaded without the copyright holder's permission, in breach of UK copyright law (Students own the copyright on schoolwork that they have produced).

This is not an exhaustive list. The school reserves the right to amend this list at any time. The headteacher or any other member of the senior leadership team will use their 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 (on the school premises and/or remotely) 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. Approval for exemptions to unblock sites may be requested in writing. The DSL and Network Manager will discuss and agree together if the site poses a safeguarding risk and subsequently whether site can be unblocked.

- Pupils may use AI tools and generative chatbots:
- 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 and staff code of conduct.

All unacceptable activity will be investigated, and subsequent education/sanction will be put into place.

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

5.1 Access to school ICT facilities and materials

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

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

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

Staff who have access to files that they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the IT support team by email: itsupport@kmingsmead.org

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. Staff should enable multi-factor authentication on their email account(s).

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/carers 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 that contains the personal information of another person, they must inform the DFO immediately and follow our data breach procedure.

Staff must not give their personal phone number(s) to parents/carers or pupils. Staff must use phones provided by the school to conduct all work-related business.

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.

5.2 Personal use

Staff are permitted to occasionally use school ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The Headteacher or DFO may withdraw or restrict this permission at any time and at their discretion.

Personal use is permitted provided that such use:

- Does not take place during working hours, except on breaks.
- 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 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff are not permitted to use their personal devices on the school network (such as mobile phones or tablets). Any information that staff access via their own internet connection or devices must be kept secure and deleted once they are no longer a member of staff.

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/carers could see them.

Staff should take care to follow the school's guidelines on use of 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 make sure 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 Facebook accounts (see appendix 1).

5.3 Remote access

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

- Remote access is managed by the Network Manager and IT support team.
- Remote access is granted via an encrypted VPN (virtual private network) which will only accept connections from devices on the school's network domain – kingsmead.org and requires a school user account to log in.
- Remote access should be automatically granted when using a school windows laptop off-site. Should this not be the case, users may use the 'PDQ Link' client to attempt to connect or connect to 'Kingsmead remote connection' in the device's network/wireless settings.
- Remote access is automatically enabled on all staff laptops, or other laptops issued for use off site. Any member of staff or student that has such a device without remote access, or where remote access is not functioning correctly, should contact the IT support team: itsupport@kingsmead.org

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 network manager may require 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. All policies can be found on the school website here

5.4 School social media accounts

The school has two official Meta accounts. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account.

The school has guidelines for what may and must not be posted on its social media accounts. Those who are authorised to manage, or post to, the account must make sure they always abide by these guidelines.

5.5 Monitoring and filtering of the school network and use of ICT facilities

To safeguard and promote the welfare of children and provide them with a safe environment to learn, the school reserves the right to filter and monitor the use of its ICT facilities and network. This includes, but is not limited to, the filtering and monitoring of:

- Internet sites visited.
- Bandwidth usage
- Email accounts
- Telephone calls

- User activity/access logs
- Any other electronic communications

Only authorised ICT personnel may filter, inspect, monitor, intercept, assess, record, and disclose the above, to the extent permitted by law. Parent/carers are informed about the filtering and monitoring procedures in place via the Online Safety and Safeguarding policies available on the school website.

The effectiveness of any filtering and monitoring will be regularly reviewed.

Where appropriate, authorised personnel may raise concerns about monitored activity with the school's designated safeguarding lead (DSL) and network manager, as appropriate.

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.
- To meet duties as described in the school's safeguarding and online safety policies.
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation.

The trust board will regularly review the effectiveness of the school's monitoring and filtering systems.

6. Pupils

6.1 Access to ICT facilities

Facilities available for pupils to access include:

- Computers and equipment in the school's ICT suites are available to pupils only under the supervision of staff. Staff should ensure doors to classrooms containing ICT facilities are locked when not in use.
- Pupils will be provided with an account linked to the school's Microsoft Office 365 environment. This can be accessed at Login | Microsoft 365 (office.com). Subject departments may provide access to other online services as required. Pupils accessing these services while off-site must abide by the same rules as when they are at school.
- Sixth-form pupils can use the computers in designated sixth form study areas independently, for educational purposes only.

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 Assistant Headteacher in charge of behaviour.
- 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 behaviour policy will be followed) The authorised staff member should:
- If a search has taken place, it must be recorded on CPOMS to 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. A list of banned items is available in the behaviour policy.
- 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, 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 behaviour for learning team and/or DSL 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 if there is a good reason to erase data or files from a device, staff members will consider if 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 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) 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 guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy / searches and confiscation policy.

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, 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 making 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.
- Consensual or non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- 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 the school's ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and/or those they share it with are 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/carers do not have access to the school's ICT facilities as a matter of course.

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

Where parents/carers 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/carers 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.

We ask parents/carers to sign the agreement in appendix 2.

7.3 Communicating with parents/carers about pupil activity

The school will ensure that parents and carers are made aware of any online activity that their children are being asked to carry out.

When we ask pupils to use websites or engage in online activity, we will communicate the details of this to parents/carers in the same way that information about homework tasks is shared.

In particular, staff will let parents/carers know which (if any) person or people from the school pupils will be interacting with online, including the purpose of the interaction. This will be shared via the curriculum MTPs and learning journeys on the school website which is in progress.

Parents/carers may seek any support and advice from the school to ensure a safe online environment is established for their child.

8. Data security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff, and learners. It therefore takes steps to protect the security of its computing resources, data, and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cybercrime technologies.

Staff, pupils, parents/carers, and others who use the school's ICT facilities should always use safe computing practices. We aim to meet the cyber security standards recommended by the Department for Education's guidance on digital and technology standards in schools and colleges, including the use of:

- Firewalls
- Security features
- User authentication and multi-factor authentication
- Anti-malware software

8.1 Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure. We recommend the 'three random words' method for choosing passwords and that passwords should be at least twelve characters long.

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, visitors, or volunteers who disclose account or password information may have their access rights revoked.

8.2 Software updates, firewalls, and anti-virus software

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

Where updates require a device to be restarted, the restart should be performed as soon as practicable.

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 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.

All policies can be found on the school website here

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 network manager and IT support team.

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 IT Support 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 shut down completely at the end of each working day.

8.5 Encryption

The school makes sure 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 network manager.

9. Protection from cyber attacks

Please see the glossary (appendix 6) to help you understand cyber security terminology.

The school will:

- Work with trustees and the IT department 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, including how to:
    - Check the sender address in an email.
    - Respond to a request for bank details, personal information, or login details.
    - Verify requests for payments or changes to information.
- 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 (such as 360 degree safe) at least annually, 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 daily and store these backups on cloud-based backup systems.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to our cloud-based provider.

- 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.
- Make sure ICT staff conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights.
- Have a firewall in place that is switched on.
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and checking if they have the Cyber Essentials certification.
- Develop, review and test an incident response plan with the IT department including, for example, how the school will communicate with everyone if communications go down, who will be contacted and when, and who will notify Action Fraud of the incident. This plan will be reviewed and tested every 6 months and after a significant event has occurred, using the NCSC's 'Exercise in a Box'

10. Internet access

The school's wireless internet connection is secured by passwords and all connections are encrypted.

- The wireless internet connection is filtered by the same firewall as the school's wired network.
- The school provides a separate wireless connection for devices intended for use by students to allow for appropriate filtering, where this may differ from filtering for staff devices.

No filter is foolproof, the school's web filter provider is a member of the internet watch foundation (IWF) and works with the UK government counter terrorist referral unit (CITRU). The IWF & CITRU block lists are integrated into the school's web filter and updated regularly by the provider. Any inappropriate site that has not been correctly identified and blocked (or site you believe to be incorrectly blocked) by the school's filter should be reported to the IT support team: itsupport@kingsmead.org

10.1 Pupils

WiFi access is not provided for student use on personal devices.

10.2 Parents/carers and visitors

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

Authorisation will only be granted if:

- Parents/carers are working with the school in an official capacity and have not been provided with a school owned device.
- 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)

If authorisation is granted, the Wi-Fi password will be entered into the device by a member of the IT support team, who will also install the security certificates required by the school's web filter. If the

certificates are not able to be installed (e.g., the device is managed by an external organisation and the visitor's user account does not have the necessary rights) then the internet connection may not work as expected and most secure web sites (https) will be inaccessible.

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

11. Monitoring and review

The headteacher, DFO and network manager monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed annually.

The board of Trustees are responsible for reviewing/approving this policy. The DSL and Network Manager will oversee and ensure this process takes place.

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
- Data protection

Appendix 1: Facebook cheat sheet for staff

Do not accept friend requests from pupils on social media

10 points of advice for school staff on Facebook

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead.
2. Change your profile picture to something unidentifiable, or if you don't, ensure that the image is professional.
3. Check your privacy settings regularly.
4. Be careful about tagging other staff members in images or posts.
5. Don't share anything publicly that you wouldn't be just as happy showing your pupils.
6. Don't use social media sites during school hours.
7. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there.
8. Don't associate yourself with the school on your profile (e.g., by setting it as your workplace, or by 'checking in' at a school event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information.
10. Consider uninstalling the Facebook app from your phone. The app recognises Wi-Fi connections and makes friend suggestions based on who else uses the same Wi-Fi connection (such as parents or pupils)

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list.
- Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster.
- **Google your name** to see what information about you is visible to the public.
- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this
- Remember that **some information is always public**: your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender.

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/carers. 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.
- If you no longer work at the school, decline the students request and do not respond to any correspondence. Alert the school that they have continued to contact you after you have left.

A parent/carer adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
    - Responding to 1 parent/carer'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/carer'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/carer 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 Facebook or 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/carer 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.

Appendix 2: Acceptable use of the internet: agreement for parents and carers

Acceptable use of the internet: agreement for parents and carers	
Name of parent/carer: **Name of child:**	
Online channels are an important way for parents/carers to communicate with, or about, our school. The school uses the following channels: • Our official Twitter accounts. • Email and text messages for parents (for school announcements and information) • Our virtual learning platform Parents/carers may also set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp or Discord).	
When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will: • Be respectful towards members of staff, and the school, at all times. • Be respectful of other parents/carers and children. • Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure. I will not: • Use private groups, the school's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive, and the school can't improve or address issues unless they are raised in an appropriate way. • Use private groups, the school's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident. • Upload or share photos or videos on social media of any child other than my own, unless I have the permission of the other children's parents/carers	
Signed:	**Date:**

Appendix 3: Acceptable use agreement for older pupils

Acceptable use of the school's ICT facilities and internet: agreement for pupils and parents/carers	
Name of pupil:	

When using the school's ICT facilities and accessing the internet in school, I will not:
• Use them for a non-educational purpose.
• Use them without a teacher being present, or without a teacher's permission.
• Use them to break school rules.
• Access any inappropriate websites.
• Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
• Use chat rooms.
• 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.
• Share any semi-nude or nude images, videos or livestreams, even if I have the consent of the person or people in the photo/video.
• Share my password with others or log in to the school's network using someone else's details.
• Bully other people.
• Use AI tools and generative chatbots (such as ChatGPT or Google Bard):
  o During assessments, including internal and external assessments, and coursework.
  o To present AI-generated text or imagery as my own work
I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.
I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.
I will always use the school's ICT systems and internet responsibly.
I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.	

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.	
Signed (parent/carer):	**Date:**

Appendix 4: Acceptable use agreement for younger pupils

Acceptable use of the school's ICT facilities and internet: agreement for pupils and parents/carers	
Name of pupil:	
When I use the school's ICT facilities (like computers and equipment) and go on the internet in school, I will not: • Use them without asking a teacher first, or without a teacher in the room with me. • Use them to break school rules. • Go on any inappropriate websites. • Go on Facebook or other social networking sites (unless my teacher said I could as part of a lesson) • Use chat rooms. • Open any attachments in emails, or click any links in emails, without checking with a teacher first. • Use mean or rude language when talking to other people online or in emails. • Send any photos, videos or livestreams of people (including me) who aren't wearing all of their clothes. • Share my password with others or log in using someone else's name or password. • Bully other people. • Use artificial intelligence (AI) chatbots, such as ChatGPT or Google Bard, to create images or write for me, and then submit it as my own work. I understand that the school will check the websites I visit and how I use the school's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules. I will tell a teacher or a member of staff I know immediately if I find anything on a school computer or online that upsets me, or that I know is mean or wrong. I will always be responsible when I use the school's ICT systems and internet. I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.	
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.	
Signed (parent/carer):	**Date:**

Appendix 5: Acceptable use agreement for staff, trustees, volunteers and visitors

Acceptable use of the school's ICT facilities and the internet: agreement for staff, trustees, volunteers and visitors	
Name of staff member/trustee/volunteer/visitor:	
When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a 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. • 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 understand 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/trustee/volunteer/visitor):	**Date:**

Appendix 6: 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.
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.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
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.
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.

TERM	DEFINITION
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.