Kings Education Trust

Shaping Futures Together.

Acceptable Use and IT

Applies to	All schools in the trust
Policy owner	CFO
Approving body	Finance Committee
Approval date	November 2026
Review cycle	Annually
Next review due	November 2027
Version and status	1.0 Approved
Linked guidance and related policies	Online safety / social media Safeguarding and child protection Behaviour Staff discipline and conduct Data protection Remote education Mobile phone usage KET Artificial Intelligence (AI) policy Freedom of information

Summary of Changes since the last approved version

Section	Summary of change	Reason for change	Impact
Front page; sections 1, 2, 5.1, 5.3 and 12; Appendix 4	Added related-policy list and adopted KET AI policy reference; added Data (Use and Access) Act 2025 and changed section 2's KCSIE reference to 2026. Corrected introductory wording, contact route to Headteacher or CEO, email/monitoring references and Appendix 4 trustee/LAC terminology.	Update references and improve consistency, navigation and KET governance terminology.	Clearer policy links and access-query escalation. Existing AI rules retained. Section 5.8's KCSIE 2025 reference remains outstanding.
Sections 4, 5.1.1, 5.2 and 5.7	Expanded web/download, chat-room and restricted-internet rules. Added issued-device responsibilities. Made encryption of sensitive/confidential email attachments mandatory; clarified subject access requests and retrieval of emails/internet history.	Clarify acceptable use, equipment care, confidentiality and lawful monitoring arrangements.	Staff must secure and return issued devices, report incidents promptly and encrypt relevant attachments. Monitoring purposes are more explicit.
Sections 5.3, 8.2 and 8.6	Distinguished authorised personal-device access from personal storage. Added restrictions on changes to systems/data and unauthorised software; required incoming-file virus-checking through IT-approved arrangements.	Clarify approval boundaries and strengthen data and software security.	Personal storage requires express written Headteacher approval and IT-confirmed security/encryption. Software installations and file checking must follow approved arrangements.
Sections 8.7 and 9; Appendix 5	Consolidated annual cyber training and expanded topics. Broadened firewall and breach-prevention requirements. Added annual cyber risk assessment, termly/post-event reviews and named senior digital-lead oversight. Updated ten glossary definitions.	Clarify training, technical protection and risk oversight; improve understanding of cyber terminology.	Annual staff/trustee/LAC training, induction and age-appropriate pupil education; more frequent training for higher-risk data roles. Risk assessment links to the existing school review. Glossary changes add no duties.

Section	Summary of change	Reason for change	Impact
Sections 5.2, 8.1, 9 and 11	Clarified current MFA and password-management arrangements following confirmation from the Trust's IT providers, and clarified the relationship between routine operational cyber-security review and the annual school cyber-security review. Independent third-party cyber-security assurance remains under consideration. Clarified current MFA and password-management arrangements following confirmation from the Trust's IT providers, and clarified the relationship between routine operational cyber-security review and the annual school cyber-security review. Independent third-party cyber-security assurance remains under consideration.	Ensure the policy reflects current operational arrangements across the Trust while allowing for further standardisation of MFA and cyber-security assurance.	No immediate change to existing user arrangements. MFA will continue to be implemented and reviewed with IT providers; existing password controls remain managed by the relevant IT Consultant.

Contents

1. Introduction and aims 5
2. Relevant legislation and guidance 5
3. Definitions 6
4. Unacceptable use 6
5. Staff (including, trustees and LAC members, volunteers, and contractors) 8
6. Pupils 12
7. Parents/carers 14
8. Data security 15
9. Protection from cyber attacks 17
10. Internet access 18
11. Monitoring and review 19
12. Related policies 19
13. Further Information 20

1. Introduction and aims

Information and communications technology (ICT) is an integral part in the running of our trust and schools. It is a critical resource for pupils, staff (including the senior leadership team), Trustees, Local Academy Committee members (LAC), volunteers and visitors. It supports teaching and learning, and the pastoral and administrative functions of the school and trust. Please note all references in this policy to schools also applies to Kings Education Trust and all employees and Trustees.

However, the ICT resources and facilities our school and trust use could also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school and trust ICT resources for staff, pupils, parents/carers and LAC
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school and trust'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, LAC, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under KET Code of Conduct and Conduct and Discipline procedures.

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
- 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 2026
- 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

- UK Council for Internet Safety (et al.) 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 governors, 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 5 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 any web page or downloading any image, document, application, or file from the internet which could be regarded as illegal, offensive, discriminatory, in bad taste, or immoral
- 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
- Using the school's systems to participate in internet chat rooms, post on internet message boards or blogs, unless approved by authorised personnel

- 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 internet and 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

This is not an exhaustive list. The school reserves the right to amend this list at any time. The CEO, Trustees or Headteachers will use their professional judgement to determine whether any act on 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 CEO or Headteacher's discretion. If this is deemed necessary then authorisation must be agreed in writing in advance from the Headteacher or CEO.

4.2. Sanctions

Pupils and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the school's policies on Discipline and Conduct and Code of Conduct. Copies have been shared with staff and hard copies are available in the school office.

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

5.1. Access to school ICT facilities and materials

The school's IT Consultant 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 IT 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 Headteacher or CEO who will make the necessary arrangements.

5.1.1 Use of school-supplied equipment

School-issued devices, including laptops, tablets and other digital devices, are provided to support teaching, learning and the efficient running of the school and trust. All school-supplied equipment remains trust property and must be returned at the end of employment or when it is no longer required. Staff must:

- Use equipment primarily for school or trust purposes and in line with safeguarding, data protection and confidentiality policies.
- Store devices securely when not in use, particularly when travelling. Do not leave devices unattended in public places or unsecured locations.
- Protect confidentiality when working away from school, including ensuring that other people cannot read sensitive information displayed on the screen.
- Lock unattended devices with a password and follow the password requirements in section 8.1.
- Update software, operating systems and applications when prompted or as directed by the school's IT Consultant.
- Connect to school systems using approved, secure methods. When using WiFi away from school, ensure the connection is secure and avoid transmitting sensitive data over public or unsecured networks.
- Report any loss, theft, damage or compromise of a school device promptly to the school's IT Consultant, designated safeguarding lead and data protection officer.

5.2. 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. Multi-factor authentication (MFA) is enabled on staff accounts where implemented by the school's IT Consultant. Staff must follow the authentication arrangements provided. The Trust will work with its IT Consultants to ensure MFA is implemented consistently across its schools and trust accounts.

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 subject access requests from individuals under the UK GDPR and 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 must be encrypted using a strong, state-of-the-art encryption standard 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 Headteacher or Deputy Headteacher immediately and follow the 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.

5.3. 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 CEO 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 their working hours
- 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 5.7). 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 policy on the use of these. 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.

Authorisation to access school or trust systems using a personal device does not automatically permit storage on that device. Staff must not save, download or synchronise school or trust data to personal devices, personal cloud storage or personal removable storage unless the headteacher has specifically authorised that storage in writing and the IT Consultants have confirmed that appropriate security and encryption requirements are met. Authorised access must comply with section 8.6.

Staff should take care to follow the school's guidelines on use of social media (see appendix 1) and use of email (see section 5.2) to protect themselves online and avoid compromising their professional integrity.

5.4. 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).

5.5. Remote access

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

- Managed by our IT consultants
- Staff must always login using only their own credentials.
- Access can be approved by the CEO or Headteacher.

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 must take such precautions as the Trust 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.

5.6. School social media accounts

The schools may have an official Facebook,. Instagram or X account, managed by the Headteacher or their nominated representative. 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 abide by these guidelines at all times.

5.7. Monitoring and filtering of the school network and use of ICT facilities

To safeguard pupils, we operate appropriate filtering and monitoring systems.

Leadership (CEO/HT/DSL) are responsible for oversight, ensure an annual review.

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 or nominated Senior Leaders may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The school reserves the right to retrieve the contents of email messages or to check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the school, including to check compliance with this policy, recover lost messages, investigate alleged wrongdoing or comply with a legal obligation.

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

Kings Education Trustees are 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.

5.8. Use of Generative AI

Staff may only use school approved AI tools. Before deploying AI that processes personal/sensitive data, school and central staff will ensure content filtering/monitoring applies, and follow DfE Generative AI safety expectations referenced in KCSIE 2026. Microsoft CoPilot is the recommended route for AI generated material.

6. Pupils

6.1. Access to ICT facilities

- Computers and Ipads are available for pupils to use but only under the supervision of school staff.
- Pupils will be provided with their own login details which must always be used to gain access to these devices.

6.2. Search and deletion

Under the Education Act 2011, the CEO, Executive 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 CEO, Headteacher or 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 then this will be dealt with according to the schools 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. A list of banned items is available in the Behaviour Policy of each school.

- 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 CEO, Headteacher or nominated Senior Leader 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 as appropriate.

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

The school will use the KET – Behaviour Policy when considering any consequences/sanctions for non adherence to this guidance.

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. 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 cyber crime technologies.

Staff, pupils, parents/carers and others who use the school's ICT facilities should use safe computing practices at all times. 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

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.

Password policies are configured and managed by the relevant school's IT Consultant. Staff and pupils must follow the password requirements applied to their accounts and must not share passwords. Passwords must be changed or reset promptly where compromise is suspected and in accordance with the arrangements specified by the IT Consultant.

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 have these installed and be configured to perform such updates regularly or automatically.

Users should not delete, destroy or modify existing systems, programs, information or data. Users must not download or install software from external sources without authorisation from the school's IT Consultant.

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 incoming files must be virus-checked through the security arrangements approved by the school's IT Consultant before they are downloaded.

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. Kings Education trust has its own Data Policy which is available for all.

8.4. Information asset & hardware/system registers

Each school will maintain a current Information Asset Register and Hardware/Systems Register using DfE templates. The CEO/HT will confirm termly that these are up to date

8.5. 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 Solus IT or Turn it On.

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 CEO, Headteacher or next most senior staff member 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.

8.6. 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 IT Consultants.

Approval under this section must distinguish between access to school or trust systems and storage of data on personal devices, personal cloud storage or personal removable storage. Any permission to store data must be expressly authorised in writing by the headteacher and meet the security and encryption requirements confirmed by the IT Consultants, in accordance with section 5.3.

8.7. Backup & recovery

We have implemented the 3-2-1 principle: 3 copies of critical data, on 2 different media/locations, 1 of which is offline

We have registered with Police CyberAlarm, maintain a Cyber Response Plan aligned to RPA guidance, and follow the annual cyber training arrangements set out in section 9, including annual NCSC cyber training for school staff and LAC members with system access.

9. Protection from cyber attacks

Please see the glossary (appendix 5) to help you understand cyber security terminology.

The Trust will:

- Work with Headteachers and the IT department to make sure cyber security is given the time and resources it needs to make the school secure
- Provide annual cyber security training for staff, trustees and LAC members, including training during induction for new starters who join outside the annual training window, and age-appropriate cyber security education for pupils. Training will cover the topics below, 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
    - Recognise phishing and social engineering, including attempts to trick users into disclosing personal information and the risks of websites containing malware
    - Use the internet safely, protect passwords and understand multi-factor authentication
    - Keep devices physically secure, including locking unattended laptops, and understand the risks of removable storage such as USB drives
    - Know how and when to report cyber incidents, cyber attacks and data breaches
    - Apply data protection requirements. All staff will receive data protection training, with more frequent training for staff exposed to higher-risk data
- 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:

- **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 to a secure cloud facility.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to our IT Consultants and CEO.
- Make sure staff:
  - Dial into our network using a virtual private network (VPN) when working from home
  - Use multi-factor authentication where it has been implemented by the school or Trust and follow any instructions issued by the relevant IT Consultant. The Trust will work with its IT Consultants to review and plan the implementation of multi-factor authentication across staff accounts.
  - Store passwords securely and only use an IT-approved password manager where one has been provided or approved by the school's IT Consultant.
- 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
- Make sure all necessary firewalls are in place and switched on, and that all areas of the network are secured effectively
- Make sure effective cyber breach prevention measures and processes are in place, for example endpoint detection and response systems
- 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 12 months. Further details may be found in Business Continuity Plans and reviewed after any significant event has occurred, using the NCSC's 'Exercise in a Box'
- Conduct a cyber risk assessment at least annually as part of the school's existing annual cyber security review described in section 11, and revisit the assessment every term and after a significant event.
- Appoint a named digital lead from the senior leadership team to oversee the cyber risk assessment.

10. Internet access

The school's wireless internet connection is secure.

- This is filtered using a education specialist provider.
- We have separate areas for managed devices and guests.
- The filters are checked by DSL's at least half termly.
- Any issues should be reported to DSL immediately by staff/pupils/parents. An investigation will be undertaken and necessary action taken immediately to rectify this.

10.1. Pupils

Wifi is not available for pupils to use in school.

10.2. Parents/carers and visitors

Parents/carers and visitors to the school will not be permitted to use the school's WiFi unless specific authorisation is granted by the headteacher.

The headteacher will only grant authorisation if:

- Parents/carers are working with the school in an official capacity (e.g. as a volunteer or as a member of the PTA)
- Visitors need to access the school's WiFi 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 WiFi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

11. Monitoring and review

The headteacher and IT Consultants 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 every year. The Trustees are responsible for this.

Cyber governance & assurance

The Trust Board have appointed a named trustee for Compliance including cyber governance (Anthony Kent).

The Headteachers will lead an annual cyber security review in their school using the DfE's Plan technology and report progress to the LAC. Each school will maintain:

- a DfE Information Asset Register and a Hardware/Systems Asset Register;
- a tested Business Continuity & Disaster Recovery plan that explicitly covers digital technology

Cyber-security arrangements are reviewed annually as part of each school's development planning process, with input from the relevant IT Consultant. The Headteacher will ensure that identified actions are recorded, monitored and reported through the school's existing governance arrangements.

In addition to the formal annual review, the relevant IT Consultant will review cyber-security arrangements routinely as part of the ongoing IT support service. Any concerns, vulnerabilities or recommended improvements identified through these reviews will be raised with the Headteacher and/or Trust as appropriate and actions monitored through existing school or trust arrangements.

12. Related policies

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

- Online safety / Social media
- Safeguarding and child protection
- Behaviour
- Staff discipline and conduct
- Data protection policies
- Remote education
- Mobile phone usage
- KET Artificial Intelligence (AI) policy
- Freedom of information

13. Further Information

Guidance is available from: https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/cyber-security-standards-for-schools-and-colleges

Appendix 1: Facebook cheat sheet for staff

Guidelines for use of Social Media

Do not accept friend requests from pupils on social media

10 rules 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, make sure 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 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 WiFi connections and makes friend suggestions based on who else uses the same WiFi 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

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 Ivingswood Academy	
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: • Facebook – open for anyone to view • X (Twitter) • Email • Text 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). The school does not have oversight of this but would expect Parents to be mindful of the posts they make on these platforms.	
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 pupils

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

Ivingswood Academy

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 AI generated work and submit this as my own work. This would include text or imagery.

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 4: Acceptable use agreement for staff, trustees and LAC members, volunteers and visitors

Acceptable use of the school's ICT facilities and the internet: agreement for staff, trustees and LAC members, volunteers and visitors

Ivingswood Academy

Name of staff member/trustee/LAC member/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 any private business, 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/LAC member/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 viruses and other kinds of malicious software.
Breach	When your data, computer systems or networks are accessed or affected without authorisation.
Cloud	An on-demand, massively scalable service, hosted on a shared infrastructure 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	Any event that threatens the confidentiality, integrity, or availability of data within your computer network, or where the security of your system or service has otherwise been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from unauthorised 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.

TERM	DEFINITION
Hacker	Someone who uses their technology skills to gain unauthorised access to computers, systems or networks.
Malware	Malicious software. Any kind of software that can damage computer systems, networks or devices, which includes viruses, trojans or any code or content that is harmful.
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 with the end aim of fixing them.
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 or text messages sent to many people asking for sensitive information (such as bank details or passwords) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems, usually by encrypting your files, until you make a payment (a ransom) for decryption.
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.

TERM	DEFINITION
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.