**Acceptable Use of Digital Technology Policy**



|  |  |  |
| --- | --- | --- |
| **Approved by: Curriculum & Standards Committee** |  | **Date:** February 2025 |
| **Last reviewed on:** | February 2023 | |
| **Next review due by:** | February 2027 | |

Contents

[Digital Technology in the Curriculum 2](#_heading=h.3rdcrjn)

[Managing the Internet 2](#_heading=h.26in1rg)

[Use of Images and Film 3](#_heading=h.35nkun2)

[Social Media 3](#_heading=h.1ksv4uv)

[Google Classroom and other VLEs 3](#_heading=h.44sinio)

[Incident Reporting, Misuse, and Inappropriate Material 4](#_heading=h.2jxsxqh)

[Safeguarding 5](#_heading=h.z337ya)

[Unacceptable use 5](#_heading=h.3j2qqm3)

[Staff (including governors, volunteers, and contractors) 6](#_heading=h.ci3v71b4ggui)

[Pupils 8](#_heading=h.rn9qbage8xk3)

[Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers) 9](#_heading=h.1y810tw)

[Appendix 2: KS2 acceptable use agreement (pupils and parents/carers) 10](#_heading=h.4i7ojhp)

[Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors) 11](#_heading=h.2xcytpi)

# Digital Technology in the Curriculum

Digital and online resources are used extensively across the curriculum at Sinai. Pupils and staff are required to sign an Acceptable Use Agreement that acknowledges this document’s contents (Appendix 1,2,3). These documents should be emailed to parents at the start of each academic year, as a Google Form, and sent out to any new children who start midway through the year.

It is essential for guidance to be given on how these technologies are to be used appropriately on a regular and meaningful basis. As part of preparing students to ensure the appropriate use of online and digital resources the school has a framework for teaching online skills within a range of curriculum areas.

# Managing the Internet

* The school provides pupils with supervised access to internet resources (where reasonable) through the school’s fixed and mobile internet connectivity.  Filtering and monitoring systems are in place to prevent access to inappropriate websites. Any misuse that is flagged through the monitoring system (Smoothwall) is followed up swiftly.

* Pupils will be advised on the most appropriate websites and resources to use for research and data collection. Staff should preview any recommended sites before use.
* If web-based research is set for homework, specific sites might be suggested that have previously been checked by the teacher, but pupils will also be encouraged to conduct independent research.
* Pupils should only access websites and resources they know to be appropriate. If they are unsure, they should exercise caution and check with their teachers before accessing websites or resources.

# Use of Images and Film

* With the written consent of parents (on behalf of pupils), the school permits the appropriate taking of images by staff of pupils for use by the school, using the school devices.
* Staff should inform pupils before images are taken as in some instances pupils may wish to withdraw permission for images to be taken.
* Staff and pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record audio or visual images of pupils, staff and others. The exception to this is on the school residential or Shabbaton where staff can use their own device, upload to a folder on the Google Drive and then immediately delete from their personal device.

# Social Media

* Pupils and parents should not seek to ‘befriend’ any member of staff and vice versa.
* Pupils are asked to report any incidents of cyberbullying to the SLT and follow the Cyberbullying guidance in the Anti-bullying policy.
* Parents should be asked not share any photos of children on social media – they should be reminded of this at all school events e.g. class assemblies.
* The school’s official social media account is managed by the head of operations. 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.

# Google Classroom and other VLEs

Google Classroom is a Virtual Learning Environment (VLE) which provides a dynamic learning space for enhancing the curriculum through collaboration, personalisation, interactive content, assessment and real-time feedback. The use of Google Classroom, or any replacement VLE is subject to the internet and network use policies.

When using Google Classroom, or any other VLE provided, pupils should:

* Log in and out carefully using only their given network identity.
* Identify themselves honestly to other users online.
* Respect other people's views and beliefs.
* Post comments appropriate to the particular discussion.

* Enjoy the interaction with fellow students and their teachers in a friendly and intellectually stimulating environment.
* Report any abuse or problem immediately.
* Be appropriately dressed if they are uploading videos of themselves.
* Work in a communal space if they are working at home.

When using Google Classroom, or any other VLE provided, pupils should not:

* Post anything illegal, obscene or offensive.
* Log in with any username other than their own.
* Copy or forward e-mail, messages, images or files without permission.
* Use storage facilities for inappropriate or non-educational material.
* Behave in an impolite manner.

When using Google Classroom, or any other VLE provided, teachers should:

* Provide suitable material that is age-appropriate.
* Ensure that they are available to respond to children’s work and questions during the school day.
* Be appropriately dressed if they are filming themselves in videos to upload.
* Talk to the children and parents in the same respectful manner as they would with in the school building.

# Incident Reporting, Misuse, and Inappropriate Material

* Pupils are aware of the procedures for reporting accidental access to inappropriate materials.
* Pupils are made aware that any breach must be immediately reported to a member of staff.
* Deliberate access to inappropriate materials by any pupil will lead to an investigation by the Headteacher and could possibly lead to a permanent exclusion and involvement of police for very serious offences.

# Safeguarding

* Staff understand it is their duty to support the whole-school safeguarding approach and will report any behaviour which they believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead or Headteacher.
* Staff will look out for incidents of cyberbullying or evidence of any other online concerns including cyber predators, children posting private information or sharing information that will haunt them later in life, children falling for scams or accidentally downloading Malware. Please see further information in the school’s Safeguarding Policy and Online Safety policy.

# 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.

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

This is not an exhaustive list. The school reserves the right to amend this list at any time. The headteacher 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.

**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 and staff code of conduct.

# 

# Staff

**Access to school ICT facilities and materials**

The school’s school business manager (SBM), technology lead and external IT company 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.

**Use of phones and email**

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

This email account should be used for work purposes only.

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

Staff must not share their personal email addresses with parents/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 head of operations 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.

Personal devices can be connected to the guest wifi but not the main school wifi.

**Personal use**

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. Where breaches of this policy are found, disciplinary action may be taken.

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.

**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.

# Pupils

**Access to ICT facilities**

* Chromebooks are available to pupils only under the supervision of staff
* Pupils will be provided with an account linked to the school’s virtual learning environment, which they can access from any device.

**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 following the DfE guidance [Searching, screening and confiscation: advice for schools 2022](https://www.gov.uk/government/publications/searching-screening-and-confiscation) **and/or**
* Is evidence in relation to an offence

**Volunteers, Governors and visitors**

* If volunteers, governors or visitors need to access the internet in school they can do so via the guest wifi network.
* Mobile phones must not be used in sight of any children or when walking around the school building and no pictures or videos should be taken, with the exception of class assemblies where parents/guardians are reminded not to share on social media.
* Any volunteers, governors or visitors who need to access the school network should only do so for the sole purpose that they are in school for.
* If access is required to an individual device the school office will set them up with an account that does now allow access to any school files or personal data.

# Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

|  |  |
| --- | --- |
| ACCEPTABLE USE OF THE SCHOOL’S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS | |
| **Name of pupil:** | |
| **When I use the school’s ICT systems (like computers) and get onto the internet in school I will:**   * Ask a teacher or adult if I can do so before using them * Only use websites that a teacher or adult has told me or allowed me to use * Tell my teacher immediately if:   + I click on a website by mistake   + I receive messages from people I don’t know   + I find anything that may upset or harm me or my friends * Use school computers for school work only * I will be kind to others and not upset or be rude to them * Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly * Only use the username and password I have been given * Try my hardest to remember my username and password * Never share my password with anyone, including my friends. * Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer * Save my work on the school network * Check with my teacher before I print anything * Log off or shut down a computer when I have finished using it   **I agree that the school will monitor the websites I visit and that there will be consequences if I don’t follow the rules.** | |
| **Signed (pupil):** | **Date:** |
| **Parent/carer agreement**: I agree that my child can use the school’s ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school’s ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these. | |
| **Signed (parent/carer):** | **Date:** |

# Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)

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

# Appendix 3: Staff acceptable use agreement

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