Clore Shalom School

Hugo Gryn Way, Shenley Hertfordshire WD7 9BL

Tel: 01923 855631

Clore Shalom School

School Policy for:

ICT & Acceptable Use

Version date: Autumn 2025

Review date: Autumn 2026

Author: Sophie Goldsmith

Monitoring: Governors

Headteacher's signature:

Date: Autumn 2025

Chair of Governor's signature

Date: Autumn 2025

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), governors, 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 governors
- 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 governors, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our code of conduct.

2. Relevant legislation and guidance

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

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- Education and Inspections Act 2006
- Keeping Children Safe in Education 2023
- 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 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
    - To write their homework or class assignments, where AI-generated text or imagery is presented as their own work

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Headteacher or a member of SLT 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.

- 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 activities listed above may face disciplinary action in line with the school's policies on behaviour and the staff code of conduct.

Copies of the behaviour policy and staff code of conduct are available from the school office.

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

5.1 Access to school ICT facilities and materials

The school's ICT 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 discuss this with the Headteacher first and then contact the school's ICT manager.

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) if possible.

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 Headteacher 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. In some very rare occasions, senior staff members are in Whatsapp groups with parents who are involved in volunteering, such as PTA.

The school phone 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 in partnership with the ICT manager 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 contact time, teaching hours or non-break time
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

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

Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities (see section 5.5). 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 personal device policy.

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. They should dial in using a virtual private network (VPN).

Staff can request remote access by informing out ICT manager who will arrange it via their personal laptops.

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 Headteacher may require against importing viruses or compromising system security. USB devices should not be used.

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.

5.4 School social media accounts

The school has an official Facebook and Instagram account, managed by the Headteacher. 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. Parents are offered the opportunity to opt-in or opt-out of the use of images of their children in a variety of circumstances and no pictures may be posted without checking of the list of permissions granted.

5.5 Storage of Images

We recognise that:

- Sharing photographs and films of our activities can help us celebrate the successes and achievements of our children and young people, provide a record of our activities and raise awareness of our organisation
- The welfare of the children and young people taking part in our activities is paramount.
- Children, their parents and carers have a right to decide whether their images are taken and how these may be used, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation.
- Consent to take images of children is only meaningful when children, their parents and carers understand how the images will be used and stored, and are fully aware of the potential risks associated with the use and distribution of these images, there are potential risks associated with sharing images of children online.

We seek to keep children safe by:

- Always asking for written consent from a child and their parents or carers before taking and using a child's image.
- Always explaining what images will be used for, how they will be stored and what potential risks are associated with sharing images of children.

- Making it clear that if a child or their family withdraw consent for an image to be shared, it may not be possible to delete images that have already been shared or published.
- Changing the names of children whose images are being used in our published material whenever possible (and only using first names if we do need to identify them)
- Never publishing personal information about individual children and disguising any identifying information (for example the name of their school or a school uniform with a logo)
- Making sure children, their parents and carers understand how images of children will be securely stored and for how long (including how we will control access to the images and their associated information)

Reducing the risk of images being copied and used inappropriately by:

- Only using images of children in appropriate clothing (including safety wear if necessary)
- Avoiding full face and body shots of children taking part in activities such as swimming where there may be a heightened risk of images being misused
- Using images that positively reflect young people's involvement in the activity.

Photography and/or filming for personal use:
When children themselves, parents, carers or spectators are taking photographs or filming at our events and the images are for personal use, we will publish guidance about image sharing in the event programmes and/or announce details of our photography policy before the start of the event. This includes

- Reminding parents, carers and children that they need to give consent for Clore Shalom to take and use their images
- Asking for photos taken during the event not to be shared on social media or asking people to gain permission from children, their parents and carers before sharing photographs and videos that include them
- Recommending that people check the privacy settings of their social media account to understand who else will be able to view any images they share
- Reminding children, parents and carers who they can talk to if they have any concerns about images being shared.

Photography and/or filming for by Clore Shalom:

We recognise that our staff may use photography and filming as an aid in activities such as music or drama. However, this will only be done with parental permission and using our equipment.
Children, young people, parents and carers must also be made aware that photography and filming is part of the programme and give written consent.
If we hire a photographer for one of our events, we will seek to keep children and young people safe by:

- Providing the photographer with a clear brief about appropriate content and behaviour
- Ensuring the photographer wears identification at all times
- Informing children, their parents and carers that a photographer will be at the event and ensuring they give written consent to images which feature their child being taken and shared
- Not allowing the photographer to have unsupervised access to children
- Not allowing the photographer to carry out sessions outside the event or at a child's home
- Reporting concerns regarding inappropriate or intrusive photography following our child protection procedures.

Photography and/or filming for wider use:

If people such as local journalists, professional photographers (not hired by Clore Shalom) or students wish to record one of our events and share the images professionally or in the wider world, they should seek permission in advance.
They should provide:

- The name and address of the person using the camera
- The names of children they wish to take images of (if possible)
- The reason for taking the images and/or what the images will be used for

- A signed declaration that the information provided is valid and that the images will only be used for the reasons given.

Clore Shalom will verify these details and decide whether to grant permission for photographs/films to be taken. We will seek consent from the children who are the intended subjects of the images and their parents and inform the photographer of anyone who does not give consent.
At the event we will inform children, parents and carers that an external photographer is present and ensure the photographer is easily identifiable, for example by issuing them with a coloured identification badge.
If Clore Shalom is concerned that someone unknown to us is using their sessions for photography or filming purposes, we will ask them to leave and (depending on the nature of the concerns) follow our child protection procedures.

- Storing images:
- We will store photographs and videos of children securely, in accordance with our safeguarding policy and data protection law.
- We will keep hard copies of images in a locked drawer and electronic images in a protected folder with restricted access. Images will be stored for a period of one half term except where certain images are kept in a secure folder for later use by the teacher, such as an end of year celebration or year book.
- We will never store images of children on unencrypted portable equipment such as laptops, memory sticks and mobile phones.
- Clore Shalom does not permit staff and volunteers to using any personal equipment to take photos and recordings of children. In the unusual event that a personal device is used, this will be with prior permission from both the Headteacher and the DSL. Only cameras or devices belonging to Clore Shalom should be used.

5.6 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. Filtering and monitoring is carried out by HFL, and the school browser history is checked daily. The school is alerted if a breach of the school's filtering systems is made and the system is tested by the school every half term.

The school monitors ICT use in order to:

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

Our governing board is responsible for making sure that:

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

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

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

If there is a breach of the filtering system, staff should report this to the Headteacher immediately.

See Appendix 6 for guidance on reporting online harm.

6. Pupils

6.1 Access to ICT facilities

- Computers and equipment are available to pupils, only under the supervision of staff.
- Specialist ICT equipment, such as that used for music, or design and technology, must only be used under the supervision of staff.
- Pupils are provided with an account linked to the school's virtual learning environment, which they can access from any chromebook.

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 or other devices that the authorised staff member has reasonable grounds for suspecting:

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

This includes, but is not limited to:

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

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

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Headteacher or the DSL (or deputy).

- 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, you should proceed according to the 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.
- Involve the DSL (or deputy) without delay if they believe that a search has revealed a safeguarding risk

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

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

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

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL (or deputy) or Headteacher or another member of the SLT 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

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

Sanctions, which may be applied, are set out in the schools behaviour policy which is available on our school website.

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. This is sent home electronically at the start of each academic year and is communicated to children regularly via PHSE lessons and assemblies.

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.

The ICT manager will generate passwords for teachers and pupils They will then be prompted to reset and set their own unique passwords which they must store securely. All staff will use the password manager required by the to help them store their passwords in a secure location incase pupils forget or lose their passwords.

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 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.

Our schools data protection policy can be found on our school website.

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 ICT manager in partnership with the Headteacher.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the Headteacher 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) to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the headteacher.

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

9. Protection from cyber attacks

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

The school will:

- Work with governors 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) 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 once a week automatically and store these backups on a cloud-based system/external hard drives that aren't connected to the school network.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to our ICT manager in partnership with those outlined in our cyber response plan.
- 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 a cyber-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 annually 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 secure.

- Our filtering and monitoring is provided by RM in partnership with Herts for Learning.

Be aware that filtering is not foolproof. If you encounter an inappropriate site that the filter hasn't identified, please report this to a member of the DSL team or the Headteacher. This will be then be logged and RM notified.

10.1 Pupils

- WiFi is available throughout the school for pupils to use from our school based devices. Pupils must liaise with a member of staff to request access to the WiFi.

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 ICT 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 governing board is responsible for approving this policy.

Appendix 1: Facebook cheat sheet for staff

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	
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 Facebook and Instagram page › Email/text groups for parents (for school announcements and information) › Our school website › Our virtual learning platform - Tapestry Parents/carers 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).	
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 • 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, governors, volunteers and visitors

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

Name of staff member/governor/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/governor/volunteer/visitor):	**Date:**

Appendix 6: Reporting illegal or harmful online contact

Reporting illegal or harmful online content

- Reporting harmful content found in school must go via the DSL and Headteacher. Children will be taught to report any harmful content they find directly to an adult.
- Parents have access to an our 'report harmful content' button which can be found on the school website: https://www.cloreshalom.herts.sch.uk/useful-links/

Know when to report

- If you or your child has seen something online that is illegal, upsetting or harmful, it is always best to report it. Illegal content includes sexual images of under 18s and unlawful terrorist content.
- You can also report something that may be legal but is still considered harmful such as content that includes bullying, self harm or suicide, impersonation, online abuse, threats, violence, unwanted sexual advances or pornographic content across non-adult sites.

Report to the correct place

- Depending on the content, reports needs to go to specific places for the correct support. Reporting child sexual abuse material goes to the Internet Watch Foundation. For terrorist content, visit ACT (Action Counters Terrorism). Many online platforms have reporting functions available to users. See https://reportharmfulcontent.com/report/ for specific guidelines on how to report harmful content across all well known apps and sites. Advice about reporting around specific harms can be found here: https://reportharmfulcontent.com/harms/

Encourage reporting

- Reporting is a practice that can work towards making the internet a safer place for all. Ignoring a piece of harmful online content can lead toward others experiencing harm.

Appendix 7: Mobile Phone Policy

1. Introduction and aims

At Clore Shalom we recognise that mobile phones and similar devices, including smartphones, are an important part of everyday life for our pupils, parents/carers and staff, as well as the wider school community.

Our policy aims to:

- Promote safe and responsible phone use
- Set clear guidelines for the use of mobile phones for pupils, staff, parents/carers, visitors and volunteers
- Support the school's other policies, especially those related to child protection and behaviour

This policy also aims to address some of the challenges posed by mobile phones in school, such as:

- Risks to child protection
- Data protection issues
- Potential for lesson disruption
- Risk of theft, loss, or damage
- Appropriate use of technology in the classroom

Note: throughout this policy, 'mobile phones' refers to mobile phones and similar devices.

2. Relevant guidance

This policy meets the requirements of the Department for Education's non-statutory mobile phone guidance and behaviour guidance. Further guidance that should be considered alongside this policy is Keeping Children Safe in Education.

3. Roles and responsibilities

3.1 Staff

All staff (including teachers, support staff and supply staff) are responsible for consistently enforcing this policy.

Volunteers, or anyone else otherwise engaged by the school, must alert a member of staff if they witness, or are aware of, a breach of this policy.

The Headteacher is responsible for monitoring the policy every two years, reviewing it, and holding staff and pupils accountable for its implementation.

Staff will address any questions or concerns from parents/carers quickly, and clearly communicate the reasons for prohibiting the use of mobile phones.

4. Use of mobile phones by staff

4.1 Personal mobile phones

Staff (including volunteers, contractors and anyone else otherwise engaged by the school) are not permitted to use their personal mobile phone, during contact time with children. Use of personal mobile phones must be restricted to non-contact time, and to areas of the school where pupils are not present (such as the staffroom).

There may be circumstances in which it's appropriate for a member of staff to have use of their phone during contact time for personal reasons. For instance (this list is non-exhaustive):

- For emergency contact by their child, or their child's school
- In the case of acutely ill dependents or family members

The headteacher will decide on a case-by-basis whether to allow for special arrangements.

If special arrangements are not deemed necessary, school staff can use the school office number as a point of emergency contact.

4.2 Data protection

Staff must not use their personal mobile phones to process personal data, or any other confidential school information, including entering such data into generative artificial intelligence (AI) tools such as chatbots (e.g. ChatGPT and Google Bard).

More detailed information can be found in a Data Protection policy and Acceptable Use policy.

4.3 Safeguarding

Staff must not give their personal contact details to parents/carers or pupils, including connecting through social media and messaging apps.

Staff must avoid publicising their contact details on any social media platform or website, to avoid unwanted contact by parents/carers or pupils.

Please see the Acceptable Use policy for further guidelines.

Staff must not use their personal mobile phones to take photographs or recordings of pupils, their work, or anything else which could identify a pupil. If it's necessary to take photos or recordings as part of a lesson/school trip/activity, this must be done using school equipment.

4.4 Using personal mobiles for work purposes

In some circumstances, it may be appropriate for staff to use personal mobile phones for work. Such circumstances may include, but aren't limited to:

- To issue homework, rewards or sanctions
- To use multi-factor authentication
- Emergency evacuations
- Supervising off-site trips
- Supervising residential visits

In these circumstances, staff will:

- Use their mobile phones in an appropriate and professional manner, in line with our staff code of conduct
- Not use their phones to take photographs or recordings of pupils, their work, or anything else which could identify a pupil
- Refrain from using their phones to contact parents/carers. If necessary, contact must be made via the school office

These circumstances should be discussed in advance with the Headteacher.

4.6 Sanctions

Staff that fail to adhere to this policy may face disciplinary action.

See the school's staff disciplinary policy for more information.

5. Use of mobile phones by pupils

Pupils should not bring mobile phones to school under any circumstances. Where children in Year 6 are travelling independently to and from school and parents provide them with a phone, the phone must be handed in to the school office who will keep it safe until the end of the day.

5.1 Use of smartwatches by pupils

Smartwatches that connect to the internet or enable children to text or make calls are not allowed in school. If a child owns a smart watch it may be used for counting steps and telling the time. If a child is using a smart watch for any other reason, it will be removed and returned to parents at the end of the day.

5.3 Sanctions

If a child is found to have a phone with them, it will be taken away and returned to a parent at the end of the day.

Certain types of conduct, bullying or harassment can be classified as criminal conduct. The school takes such conduct extremely seriously and will involve the police or other agencies as appropriate.

Such conduct includes, but is not limited to:

- Sexting (consensual and non-consensual sharing nude or semi-nude images or videos)
- Upskirting
- Threats of violence or assault

- Abusive calls, emails, social media posts or texts directed at someone on the basis of someone's ethnicity, religious beliefs or sexual orientation

6. Use of mobile phones by parents/carers, volunteers and visitors

Parents/carers, visitors and volunteers (including governors and contractors) must adhere to this policy as it relates to staff if they are on the school site during the school day.

This means:

- Not taking pictures or recordings of pupils, unless it's at a public event (such as a school fair), or of their own child
- Using any photographs or recordings for personal use only, and not posting on social media without consent
- Not using phones in lessons, or when working with pupils

Parents/carers, visitors and volunteers will be informed of the rules for mobile phone use when they sign in at reception or attend a public event at school.

Parents/carers or volunteers supervising school trips or residential visits must not:

- Use their phone to make contact with other parents/carers
- Take photos or recordings of pupils, their work, or anything else which could identify a pupil

Parents/carers or volunteers supervising trips are also responsible for enforcing the school's policy for pupils using their phones, as set out in section 5 above, but must refer any sanctions to a member of staff, as they do not have the power to search or confiscate devices.

Parents/carers must use the school office as the first point of contact if they need to get in touch with their child during the school day. They must not try to contact their child on their personal mobile during the school day.

7. Loss, theft or damage

The school accepts no responsibility for mobile phones that are lost, damaged or stolen on school premises or transport, during school visits or trips, or while pupils are travelling to and from school.

Confiscated phones will be stored in the the school office in a locked cabinet and can only be collected by a parent. They will not be handed back to children at the end of the day.

8. Monitoring and review

The school is committed to ensuring that this policy has a positive impact of pupils' education, behaviour and welfare. When reviewing the policy, the school will take into account:

- Feedback from parents/carers and pupils
- Feedback from staff
- Records of behaviour and safeguarding incidents
- Relevant advice from the Department for Education, the local authority and any other relevant organisations

9.Acceptable Use Agreement for pupils allowed to bring their phones to school due to exceptional circumstances

You must obey the following rules if you bring your mobile phone to school:

- You may not use your mobile phone during lessons, unless the teacher specifically allows you to.
- Phones must be switched off (not just put on 'silent').
- You may not use your mobile phone in the toilets or changing rooms. This is to protect the privacy and welfare of other pupils.
- You cannot take photos or recordings (either video or audio) of school staff or other pupils without their consent.
- Avoid sharing your contact details with people you don't know, and don't share other people's contact details without their consent.
- Don't share your phone's password(s) or access code(s) with anyone else.
- Don't use your mobile phone to bully, intimidate or harass anyone. This includes bullying, harassing or intimidating pupils or staff via:
    - Email
    - Text/messaging app
    - Social media
- Don't use your phone to send or receive anything that may be criminal. For instance, by 'sexting'.
- Rules on bullying, harassment and intimidation apply to how you use your mobile phone even when you aren't in school.
- Don't use vulgar, obscene or derogatory language while on the phone or when using social media. This language is not permitted under the school's behaviour policy.
- Don't use your phone to view or share pornography or other harmful content.
- You must comply with a request by a member of staff to switch off, or hand over, a phone. Refusal to comply is a breach of the school's behaviour policy and will be dealt with accordingly.
- Mobile phones are not permitted in any internal or external exam or test environment. If you have a mobile phone, you will be asked to store it appropriately, or turn it over to an exam invigilator, before entering the test room. Bringing a phone into the test room can result in your exam being declared invalid.

10. Permission form allowing a pupil to bring their phone to school

PUPIL DETAILS	
Pupil name:	
Year group/class:	
Parent/carer(s) name(s):	

The school has agreed to allow (Pupils name) to bring their mobile phone to school because they:

- Travel to and from school alone
- Are a young carer
- Need the phone to support their medical needs
-

Pupils who bring a mobile phone to school must abide by the school's policy on the use of mobile phones, and its code of conduct/acceptable use agreement.

The school reserves the right revoke permission if a pupil does not abide by the policy.

Parent/carer signature: _____

FOR SCHOOL USE ONLY	
Authorised by:	
Date:	

11. Template mobile phone information slip for visitors

Use of mobile phones and similar devices in our school

- Please keep your mobile phone on silent/vibrate while on the school grounds
- Please do not use phones where pupils are present. If you must use your phone, you may go to the staff room.
- Do not take photos or recordings of pupils (unless it is your own child), or staff
- Do not use your phone in lessons, or when working with pupils

The school accepts no responsibility for phones that are lost, damaged or stolen while you are on the school grounds.

A full copy of our mobile phone policy is available from the school office.

Appendix 8: 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.