



Chawson First School

ICT and internet acceptable use policy

Reviewed by:	Lindsay Wood	Date: March 2026
Next review due:	March 2027 (Ideally annually)	

1. Introduction and aims	2
2. Relevant legislation and guidance	2
3. Definitions	3
4. Unacceptable use	3
5. Staff (including governors, volunteers, and contractors)	4
6. Children	8
7. Parents/carers	10
8. Data security	11
9. Protection from cyber attacks	12
10. Internet access	13
11. Monitoring and review	14
12. Related policies	14
Appendix 1: Facebook cheat sheet for staff	15
Appendix 2: Acceptable use of the internet: agreement for parents and carers	17
Appendix 3: Acceptable use agreement for children	18
Appendix 4: Acceptable use agreement for staff, governors, volunteers and visitors	20
Appendix 5: Glossary of cyber security terminology	21

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 children, 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, children, 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 children safe and effective internet and ICT use

This policy covers all users of our school's ICT facilities, including governors, staff, children, volunteers, contractors and visitors **and anyone who has access to our IT and communication systems.**

Breaches of this policy may be dealt with under our staff 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](#)
- [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 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, children, 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, 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 children, 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 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):
 - where AI-generated text or imagery is inappropriate

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

4.1 Exceptions from unacceptable use

Where the use of school ICT facilities (on the school premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the Headteacher's discretion. Should staff need to gain permission for such activity they must do so before the event from the Headteacher

Acceptable use of artificial intelligence (AI) tools here, may be acceptable for example:

- Under the direction of staff, children may use AI tools and generative chatbots to complete lesson activities:
- 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

Children 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/safeguarding/staff code of conduct.

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

5.1 Access to school ICT facilities and materials

The school's network manager/ computing lead/school business manager (SBM) 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 for the first time. Staff will then be prompted to change the password to a secure one as specified in section 8.1.

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 school's network manager/ computing lead/school business manager (SBM).

School-issued devices (including laptops, tablets and other digital devices) are provided to staff for the purpose of supporting teaching, learning and the efficient running of the school. All school-supplied equipment remains the property of the school and staff must return the equipment at the end of employment, or when it is no longer required. Staff must:

- Use equipment and devices primarily for school purposes and in line with the school's policies on safeguarding, data protection and confidentiality
- Store devices securely when not in use, particularly when travelling. Devices should not be left unattended in public places or in unsecured locations
- Be actively aware of data security and confidentiality and follow best practice when accessing the equipment away from school. E.g. when travelling on public transport, be aware that other passengers may be able to read any documents displayed on the screen of your device
- Ensure devices lock with a password when unattended. Passwords must:
 - Not be shared with others and must be changed regularly
 - Be suitably strong, in accordance with the school's password policy (see section [8.1])
- Update software, operating systems and applications when prompted, or as directed by the [ICT manager]
- Connect to the school network using approved and secure methods. When connecting to wi-fi networks outside of the school, staff must ensure connections are 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 [ICT manager], designated safeguarding lead and data protection officer

5.1.1 Use of phones/ smart watches and email

School phones must not be used for personal matters except for emergency use of office phones.

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.

Personal mobile phones

Staff (including volunteers, contractors and anyone else otherwise engaged by the school) are not permitted to use their personal mobile phone, while children are present/during contact time. 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/ PPA room).

There may be circumstances in which it's appropriate for a member of staff to have access to 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
- When expecting a medical call

The Headteacher will decide on a case-by-case 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.

Smart watches

Smart watches are now devices with communications and smart technology similar to that of mobile phones. This includes smartwatches that have the capability to send and receive text and voice messages, make calls and listen to music, and access sent images. As such use of these features during school hours is restricted as per the use of personal mobile phones. Staff should abide by the same rules and disable features/ Bluetooth connections which could cause distraction during lesson times or pose a safeguarding concern by possibly exposing children to viewing inappropriate adult content.

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 children, and must not send any work-related materials using their personal email account. In the event that email correspondence with parents is needed emails should be sent via the school office or through year group emails – not their individual school email account. The exception to this is the Senior Leadership team who may wish to communicate with parents directly.

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, sent to secure email addresses or be password protected with the password sent separately or given verbally 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 children. Staff must use phones provided by the school to conduct all work-related business unless permission has been given to use own equipment with caller ID blocked, such as the need for telephone parent's consultation.

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

Staff when working with a school-provided laptop at home may also use it for limited personal use as would be permitted in school. They must however not use it to store to store personal non-work-related information or materials (such as music, videos, or photos).

Staff should be aware that this use can be monitored even when offsite and their attention drawn to the fact that the use of the school's ICT facilities either in school or at home 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 may use personal ICT equipment to plan, and access school emails such as a home PC or mobile phones. Any documents that contain personal information must not be saved to personal devices, As per GDPR policy. Documents may be worked on or new documents uploaded to the server using Foldr or must be transported on an encrypted memory stick. Staff must ensure that any equipment they use has sufficient up to date anti-virus protection to restrict the possibility of infecting the school computer systems.

Staff are also permitted to use their personal devices (such as mobile phones) in line with the school's mobile phone policy. Staff may use their phone, where it is necessary for teaching, once they have consulted with the Headteacher to confirm its use. This has become necessary when staff need to stream music to our mobile Bluetooth speakers. Other authorised uses may come to light as technology changes but recording images of children is still prohibited.

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 children 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. **Staff must ensure that multi-factor authentication is used.**

Teaching staff can access the schools' server and saved resources via the internet remotely. Any teacher may use their personal login to access through a website called Foldr. Teachers may access the server with the same level of clearance that they have when in school. Files can be worked on and saved onto the server without needing to download them. Files may be retrieved and saved locally but these should not contain personal data unless they are encrypted or saved to the school laptop provided. New files can also be created and saved to the server avoiding the need to transfer files on portable memory sticks.

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 take such precautions and are required to connect devices in school regularly to keep them updated and protect 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.

Our school data protection policy is available on the school website.

5.4 School social media accounts

The school has an official Facebook account, managed by members of the senior leadership team. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account.

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

To comply with Department for Education (DfE) guidance on [meeting digital and technology standards](#), and 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. As a school we have a Service Level Agreement with Entrust who provide the school with a designated ICT technician. Aspects of school's technical infrastructure and internet safety are delegated to the technician who is managed by the ICT lead.

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 for the following purposes (amend as necessary):

- To monitor whether the use of the email system or the internet is legitimate and in accordance with this policy
- To find lost messages or retrieve messages lost due to computer failure
- To help in the investigation of alleged wrongdoing
- To comply with any legal obligation

The list above is not exhaustive.

The school monitors ICT use in order to:

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

Our governing board is responsible for making sure that:

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

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

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

6. Children

6.1 Access to ICT facilities

Computers and equipment in the school's ICT suite are available to children only under the supervision of staff

Children are also able to use laptops and ipads in the classroom, again always under supervision.

The DfE's non-statutory mobile phone guidance says that children should not use mobile phones throughout the school day. It is therefore school policy that children do not bring mobile phones or other such devices with communications and smart technology. This includes smartwatches with smart technology in them which can be used to tell the time, send and receive text and voice messages, make calls and listen to music, have wellness and health-related features.

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 children 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 children, **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 children and staff. If the search is not urgent, they will seek advice from the Headteacher / DSL / appropriate senior leadership member
- Explain to the Child 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 Child's co-operation

The authorised staff member should:

- 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 DSL / Headteacher / other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

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

- They reasonably suspect that its continued existence is likely to cause harm to any person, **and/or**
- The Child 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 children 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 and or the online safety policies

Any complaints about searching for, or deleting, inappropriate images or files on children's 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 children, in line with the behaviour/ online safety policy, if a child 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 children, 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

Where a child misuses the school's ICT systems or internet, we will deal with the incident as soon as possible following the relevant procedures set out in our policies on safeguarding, behaviour, online safety and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

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 children, 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 Child 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 children 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 children 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, children, 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 and confidential. Strong passwords should be at least 8 characters, with a combination of upper and lower-case letters and numbers and symbols.

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 children 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 technician will generate passwords for children and these are kept in a secure location on the school system in case children lose or forget their passwords by the ICT lead.

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. This will be completed by the ICT technician following authorisation from the ICT lead or Headteacher.

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.

The school's Data Protection Policy can be found on the 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 school ICT technician under the direction of the Headteacher/ ICT lead or school business manager.

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

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

8.5 Encryption

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

School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as Child 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 technician/ Headteacher/ ICT lead or school business manager

9. Protection from cyber attacks

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

The school will:

- Work with governors and the ICT lead 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
 - Online safety and password security
 - Social engineering, including not using websites that host unsuitable material, and could also contain malware and viruses
 - The physical security of devices, for example not leaving a laptop unlocked and unattended
 - The risks of using removable storage media, such as USBs
 - Multi-factor authentication
 - How and when to report a cyber incident or attack
 - How and when to report a data breach
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether our IT software needs updating or replacing to be more secure

- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Put controls in place that are:
 - **Proportionate:** the school will verify this using a third-party audit (such as [360 degree safe](#)) at least annually, to objectively test that what it has in place is effective
 - **Multi-layered:** everyone will be clear on what to look out for to keep our systems safe
 - **Up to date:** with a system in place to monitor when the school needs to update its software
 - **Regularly reviewed and tested:** to make sure the systems are as effective and secure as they can be
- Back up critical data as an automatic process which is monitored by the ICT technician weekly and store these backups on cloud-based backup systems/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 Entrust through and SLA agreement.
- Make sure staff:
 - Dial into our network using a virtual private network (VPN) Folder, when working from home
 - Enable multi-factor authentication where they can, on things like school remote access and email accounts
 - Use secure passwords and store them securely
- Make sure ICT staff conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
- Have a firewall in place that is switched on
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and checking if they have the [Cyber Essentials](#) certification
- Develop, review and test an incident response plan with the IT department including, for example, how the school will communicate with everyone if communications go down, who will be contacted and when, and who will notify [Action Fraud](#) of the incident. This plan will be reviewed and tested at least annually and after a significant event has occurred, using the NCSC's '[Exercise in a Box](#)'
- Work with our Local Authority to see what it can offer the school regarding cyber security, such as advice on which service providers to use or assistance with procurement
- **Conduct a cyber risk assessment at least annually, or after a significant event has occurred**

10. Internet access

The school's wireless internet connection is secure and the Wifi password is only known to authorised members of the Senior leadership team.

It is accessible on all school devices by staff and children. Filters provided by our internet provider restrict access to unblocked sites e.g social media. Any inappropriate sites that may accidentally get past a filter are the responsibility of all to reporting to the ICT Lead. In addition, sites that staff believe need to be accessed but have been blocked can be discussed with SLT so that they may be made available.

Personal access to the Wi-Fi is available to staff on personal devices such as mobile phones through a guest login. This is monitored as the schools main wifi connection.

10.1 Children

Children only have access to the internet when using it in lessons under the supervision of an adult. Children learn about online-safety as part of their curriculum. The school has filters that should restrict access to unsuitable material. However, in the event that they do not block all this material children are taught to report anything that they should see that they feel unsure about when using the internet for research to the adult supervising the session.

10.2 Parents/carers and visitors

Parents/carers and visitors to the school will not be permitted to use the school's main WiFi but will have access to a guest wifi authorised 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)
- Parents/carers need Wifi access to make payments for items on school property
- 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 /ICT technician/ ICT lead and SBM, 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 3 years and approved by the governing board.

12. Related policies

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

- Online safety
- Safeguarding and child protection
- Behaviour
- Staff code conduct
- Data protection

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 children
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, our school or your children 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 children)

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, children 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 Child adds you on social media

- In the first instance, ignore and delete the request. Block the Child from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture

- If the Child asks you about the friend request in person, tell them that you're not allowed to accept friend requests from children and that if they persist, you'll have to notify senior leadership and/or their parents/carers. If the Child 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
 - Children 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 Child 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/carers: _____		
Name of child: _____		Class: _____
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 page • Email/text groups for parents (for school announcements and information) • 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 if they aren't 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 other children's parents/carers		
Signed:		Date:

Appendix 3: Acceptable use agreement for children



Acceptable use of the school's ICT facilities and internet: agreement for KS2 children



Class:

Date:

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 usernames 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 that might upset, distress or harm me or others
- Always log off or shut down a computer when I've finished working on it

I will not:

- 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
- Create, link to or post any material that is offensive or otherwise inappropriate
- 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 agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (child):

Date:



Acceptable use of the school's ICT facilities and internet: agreement for EY/KS1 children



Class:

Date:

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 select 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
- 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 (children):

Date:

 Acceptable use of the school's ICT facilities and internet: agreement for staff, governors, volunteers and visitors 	
Name of staff member/governor/volunteer/visitor: _____	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way that could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of children without checking with teachers first • Share confidential information about the school, its children 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 child informs me they have found any material that 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 children in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	Date:

Appendix 5: Glossary of cyber security terminology

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

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove 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.
Hacker	Someone who uses their technology skills to gain unauthorised access to computers, systems and 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.

TERM	DEFINITION
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's of use to an attacker.
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.



Acceptable use for trips and visits: agreement for parents and carers



At Chawson First School we encourage parents to volunteer to support on school trips and visits and need to ensure that safeguarding of the children is a priority at all times. To ensure this we have to make sure any risks are managed and kept to a minimum, for the safety and health of all individuals on the trip at all times.

In partnership with this we ask that you read and sign this document to agree to following the points below to ensure safety for all.

Before attending the visit:

- I will read through the provided risk assessment and ask for any points to be explained if they are not fully clear.

During the visit I will:

- Be respectful towards members of staff, and the children, at all times.
- Follow the direction and instruction of the class teacher.
- Not leave the group at any time without having spoken to the class teacher.
- Ensure that my phone is kept away during the visit and whilst on the coach.
- Not take any photographs of any children at any time – I understand staff will have this responsibility using school devices.

In the event of needing to be contacted for emergency purposes I will;

- Inform the class teacher,
- Keep my phone on silent,
- Use my phone away from the main group after alerting a member of staff at a time that does not compromise the safety of the children under your supervision.

Signed:

Date:

Name of parent/carers: _____

Name of child: _____

Class: _____