ICT and Internet Acceptable Use Policy

October 2023

Policy No: 87

DATE APPROVED BY GOVERNING BODY: 16.10.2023

DATE OF NEXT REVIEW: Autumn 2026

Lead: Angela Macvie

Governor Responsible: Governing Body

Contents

1. Introduction and Aims

1.1. 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.

1.2. However, the ICT resources and facilities Chadsgrove uses could also pose risks to data protection, online safety and safeguarding.

1.3. This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, Parent 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

1.4. Breaches of this policy may be dealt with under the Disciplinary Procedures and Staff Code of conduct.

2. Relevant Legislation and Guidance

2.1. 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

3.1. The following definitions are used in the context of this policy:

- **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

3.2. See Appendix 7 for a glossary of cyber security terminology.

4. Unacceptable Use

4.1. 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).

4.2. 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, anti-Semitic or discriminatory in any other way
- Using Artificial Intelligence (AI) tools and generative chatbots (such as ChatGPT and Google Bard):
    - During assessments, including internal and external assessments, and coursework
    - To write their homework or class assignments, where AI-generated text or imagery is presented as their own work

4.3. This is not an exhaustive list. The school reserves the right to amend this list at any time. The Headteacher or any other relevant member of staff 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.

Exceptions from Unacceptable Use

4.4. 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. This would need to be requested via a conversation with the Headteacher, the outcome of which would need to be recorded.

4.5. Pupils may use Artificial Intelligence (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 ICT lessons or art homework about AI-generated images. All AI-generated content must be properly attributed

Sanctions

4.6. 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, Discipline and the staff code of conduct, all of which can be found on the Staff Share area of the school network

5. Staff (including Governors, Volunteers, and Contractors)

Access to School ICT Facilities and Materials

5.1. Chadsgrove's ICT manager, in liaison with the Senior Leadership Team, manages access to the school's ICT facilities and materials for school staff. This includes, but is not limited to:

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

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

5.3. 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 a member of the Senior Leadership Team.

Use of Phones and Email

5.4. Chadsgrove provides each member of staff with an email address that is accessed via multi-factor authentication. This email account should be used for work purposes only.

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

5.6. Staff must not share their personal (non-work) email addresses with Parent Carers or pupils, and must not send any work-related materials using their personal email account.

5.7. 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.

5.8. 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.

5.9. 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.

5.10. If sending an email to several parent carers at the same time, 'BCC' or Arbor, the school's management information system should be used in order to prevent the sharing of private email addresses

5.11. 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.

5.12. If staff send an email in error that contains the personal information of another person, they must inform a member of the Senior Leadership Team immediately and follow the data breach procedure.

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

5.14. Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use. School phones must not be used for personal matters.

5.15. Chadsgrove is currently considering recording incoming and outgoing phone conversations. Should phone calls be recorded, callers will be made aware that the conversation is being recorded and the reasons for doing so – for example, calls to the school office may be recorded to aid administrators or calls may be recorded for use in staff training.

5.16. Staff who would like to record a phone conversation should speak to a member of the Senior Leadership Team. All non-standard recordings of phone conversations must be pre-approved and consent obtained from all parties involved.

5.17. Requests to record conversations may be granted when:

- Discussing a complaint raised by a Parent Carer or member of the public
- Calling Parent Carers to discuss behaviour or sanctions
- Taking advice from relevant professionals regarding safeguarding, special educational needs (SEN) assessments, etc.
- Discussing requests for term-time holidays

This list is not exhaustive

Personal Use

5.18. 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. Any member of the School Leadership Team may withdraw or restrict this permission at any time and at their discretion.

5.19. Personal use is permitted provided that such use:

- Does not constitute 'unacceptable use', as defined above
- Takes place during break/non-contact times and 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

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

5.21. Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities. Where breaches of this policy are found, disciplinary action may be taken.

5.22. Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the school's Mobile Phone Policy.

5.23. 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 Parent Carers could see them.

5.24. 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) to protect themselves online and avoid compromising their professional integrity.

Personal Social Media Accounts

5.25. Members of staff should make sure their use of social media, either for work or personal purposes, is appropriate at all times.

5.26. Chadsgrove has guidelines for staff on appropriate security settings for Facebook accounts (see Appendix 1).

Remote Access

5.27. Chadsgrove allows named/authorised members of staff to access the school's ICT facilities and materials remotely. This is managed by the ICT manager in liaison with the Senior Leadership Team.

5.28. Members of staff are required to authenticate in order to log on to the remote desktop using their usual access credentials.

5.29. Non-authorised members of staff requiring remote access should request this from a member of the Senior Leadership Team.

5.30. 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 required against importing viruses or compromising system security.

5.31. Chadsgrove ICT facilities contain information that is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with the data protection policy. This can be found on the staff share area of the school network.

School Social Media Accounts

5.32. Chadsgrove has an official 'X', (formerly known as Twitter) account. Staff members, who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account.

5.33. 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.

6. Pupils

Access to ICT facilities

6.1. Computers and equipment in the school's ICT suite are available to pupils only under the supervision of staff, unless specific permission has been granted. Post 16 pupils can use the computers in the ICT room independently, for educational purposes only.

6.2. Specialist ICT equipment, such as that used for music, must only be used under the supervision of staff.

6.3. Where appropriate, pupils are provided with an account linked to the school's virtual learning environment, which they can access from any device by using the following URL- https://chadsgrove.eschools.co.uk/login.

Search and Deletion

6.4. Under the Education Act 2011, the Headteacher, and any member of staff authorised to do so by the Headteacher (and trained appropriately in how to search lawfully and safely), can search pupils and confiscate their mobile phones, computers or other devices that the authorised staff member has reasonable grounds for suspecting:

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

This includes, but is not limited to:

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

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

- Assess 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 member of the Senior Leadership Team
- 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, staff will proceed according to the behaviour policy.

6.6. The authorised staff member will:

- Inform the Headteacher/DSL (or deputy) of any searching incidents where they had reasonable grounds to suspect a pupil was in possession of a banned item. A list of banned items is available in the Behaviour Policy.
- Involve the Headteacher/DSL (or deputy) without delay if they believe that a search has revealed a safeguarding risk

6.7. 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.

6.8. 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

6.9. If inappropriate material is found on the device, it is up to the Headteacher 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.

6.10. 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 Carer refuse to delete the material themselves

6.11. 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

6.12. 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
- The school's Behaviour Policy

6.13. Any complaints about searching for, or deleting, inappropriate images or files on pupils' devices will be dealt with through the school complaints procedure.

Unacceptable use of ICT and the internet outside of school

6.14. Chadsgrove will sanction pupils, in line with the Behaviour Policy if a pupil engages in any of the following **at any time** (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or making statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Consensual or non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other pupils, or other members of the school community
- Gaining or attempting to gain access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to the school's ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and/or those they share it with are not supposed to have access, or without authorisation
- Using inappropriate or offensive language

7. Monitoring and Filtering of the School Network and Use of ICT Facilities

7.1. Chadsgrove 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

7.2. Only the ICT Manager and Designated Safeguarding Leads may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law. Senso Cloud is used for the purposes of monitoring internet use.

7.3. Chadsgrove monitors ICT use in order to:

- Safeguard and promote the welfare of children and provide them with a safe environment to learn
- 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

7.4. The Governing Body 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

7.5. Chadsgrove's Deputy Designated Safeguarding Lead, under the direction of the Designated Safeguarding Lead takes lead responsibility for understanding the filtering and monitoring systems and processes in place.

7.6. Where appropriate, staff may raise concerns about monitored activity with the Headteacher/ DSL as appropriate.

8. Parent Carers

Access to ICT Facilities and Materials

8.1. Parent Carers do not have access to the Chadsgrove's ICT facilities as a matter of course. However, Parent Carers working for, or with, the school in an official capacity (for instance, as a volunteer) may be granted an appropriate level of access, or be permitted to use the school's facilities at the Headteacher's discretion.

8.2. Where Parent Carers are granted access in this way, they must abide by this policy as it applies to staff.

Communicating With or About the School Online

8.3. Chadsgrove believes that it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online.

8.4. Parent 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.

8.5. Chadsgrove asks Parent Carers to sign the agreement in Appendix 2.

Communicating with Parent Carers about Pupil Activity

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

8.7. When school staff ask pupils to use websites or engage in online activity, we will communicate the details of this to Parent Carers in the same way that information about homework tasks is shared.

8.8. In particular, staff will let Parent Carers know which (if any) person or people from the school pupils will be interacting with online, including the purpose of the interaction.

8.9. Parent Carers may seek any support and advice from the school to ensure a safe online environment is established for their child.

9. Data Security

9.1. Chadsgrove 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.

9.2. Staff, pupils, Parent Carers and others who use the school's ICT facilities are expected to use safe computing practices at all times. The school aims 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

Passwords

9.3. All users of Chadsgrove's ICT facilities are expected to set strong passwords for their accounts and keep these passwords secure.

9.4. Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

9.5. Members of staff or pupils who disclose account or password information may face disciplinary action. Parent Carers, visitors or volunteers who disclose account or password information may have their access rights revoked.

Software updates, firewalls and anti-virus software

9.6. All of Chadsgrove's ICT devices that support software updates, security updates and anti-virus products have these installed, and are configured to perform such updates regularly or automatically.

9.7. 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.

9.8. Any personal devices using the school's network must all be configured in this way.

Data Protection

9.9. All personal data is processed and stored in line with data protection regulations and the school's Data Protection policy that can be found on the staff share area of the school network.

Access to Facilities and Materials

9.10. All users of the Chadsgrove l's ICT facilities will have clearly defined access rights to school systems, files and devices.

9.11. These access rights are managed by the ICT Manager in liaison with the Senior Leadership Team.

9.12. 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 a member of the Senior Leadership Team immediately.

9.13. Users are expected to 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.

Encryption

9.14. Chadsgrove makes sure that its devices and systems have an appropriate level of encryption.

9.15. School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the Headteacher.

9.16. 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 in liaison with the Senior Leadership Team.

10. Protection from Cyber Attacks

10.1. Chadsgrove will:

- Work with Governors and the ICT Manager 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 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 yearly 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 school 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 three times a day and store these backups on a cloud-based backup system which isn't connected to the school network.
- Delegate specific responsibility for maintaining the security of the school's management information system (MIS) to Arbor
- Make sure staff:
    - Enable multi-factor authentication where they can, on things like school email accounts
    - Store passwords 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 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 the 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

11. Internet Access

11.1. Chadsgrove's wireless internet connection is secure.

11.2. Filtering is in place on the school network, though it is recognised that filters are not fool proof. Staff are expected to report any inappropriate sites that the filter hasn't identified (or appropriate sites that have been filtered in error) to a member of the Senior Leadership Team immediately.

11.3. Parent Carers and visitors to the school will not be permitted to use the school's Wi-Fi unless specific authorisation is granted by the Headteacher or member of the Senior Leadership Team.

11.4. The Headteacher will only grant authorisation if:

- Parent Carers are working with the school in an official capacity (e.g. as a volunteer)
- Visitors need to access the school's Wi-Fi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

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

12. Monitoring and Review

12.1. The Headteacher and ICT Lead review and monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.

12.2. This policy will be reviewed every three years.

13. Related Policies

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

- Behaviour (Policy Number 56)
- Safeguarding and Child Protection (Policy Number 73)
- Disciplinary Procedure (Policy Number 83)
- Data protection (Policy Number 84)
- School Systems and data Security (Policy Number 85)
- Remote Learning (Policy Number 111)
- Mobile Phone (Policy Number 112)

Appendix 1: Facebook and Social media Advice for Staff

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 Wi-Fi connections and makes friend suggestions based on who else uses the same Wi-Fi connection (such as Parent Carers 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**

- 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

- 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 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 Parent 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

You receive a friend request from a Parent Carer

- Please do not respond to friend request from Parent Carers:
  - Responding to one 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
- Check your privacy settings and consider changing your display name or profile picture
- Notify a member of the Senior Leadership Team or the Headteacher about what's happening

You are 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, the school's 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 will 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 Parent Carers

Acceptable Use of the Internet: Agreement for Parent Carers	
Name of Parent Carer: **Name of Pupil:**	
Online channels are an important way for Parent Carers to communicate with, or about, our school. The school uses the following channels: • Emails from individual school staff • Arbor (our Management Information System) to send emails and texts to individuals or groups of Parent Carers On occasions, Parent Carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, 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 Parent Carers and pupils • 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 schools 'X' (Twitter), 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 schools 'X' (Twitter), 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 pupil other than my own, unless I have the permission of the other pupil's Parent Carers	
Signed:	**Date:**

Appendix 3: Acceptable Use Agreement for Older Pupils on the Formal Pathway

Acceptable use of the school's ICT facilities and internet:
Agreement for pupils and Parent 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 allowed this as part of a learning activity)
- Use chat rooms
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Share any semi-nude or nude images, videos or livestreams, even if I have the consent of the person or people in the photo/video
- Share my password with others or log in to the school's network using someone else's details
- Bully other people
- Use Artificial Intelligence tools (AI) and generative chatbots (such as ChatGPT or Google Bard):
    - During assessments, including internal and external assessments, and coursework
    - To present AI-generated text or imagery as my own work

I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the school's ICT systems and internet responsibly.

I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.

Signed (pupil):	**Date:**

Parent Carer agreement:
I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (Parent Carer):	**Date:**

Appendix 4: Acceptable use agreement for younger pupils on the Formal pathway

Acceptable use of the school's ICT facilities and internet: agreement for pupils and Parent 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 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:**

Acceptable use of the school's ICT facilities and internet: Agreement for pupils and Parent Carers	
Name of pupil:	
When using the school's ICT facilities and accessing the internet in school, I will: • Ask an adult if I want to use the computer • Only use activities on the computer if an adult says it is OK • Take care of the computer and other equipment • Ask for help from an adult if I am not sure what to do or if I think I have done something wrong • Turn off the monitor and tell an adult if I see something that upsets me on the screen I know that if I break the rules I might not be allowed to use a computer. I understand that my teachers will look at what I am doing on the computer 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 6: 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 • Open any attachments in emails, or follow any links in emails, if the sender is not known or the email is not expected	
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 7: 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.
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.

TERM	DEFINITION
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 that 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.