WHITE HOUSE SCHOOL

ICT and Internet Acceptable Use Policy

Prepared by: Elle Vinall
Date: September 2026

CAVENDISH EDUCATION

Contents:

1. Context 3
2. Aims 4
3. Legislation and Guidance 4
4. Definitions 5
5. Unacceptable Use 6
6. Staff 7
7. Pupils 11
8. Parents and Carers 14
9. Data Security 14
10. Protection from Cyber Attacks 16
11. Internet Access 17
12. Monitoring Arrangements 17
13. Links with other policies 18

Appendix 1: Facebook Cheat Sheet for Staff
Appendix 2: Acceptable Use of the Internet – Agreement for Pupils and Parent/Carers
Appendix 3: Acceptable Use of the Internet – Agreement for Staff and Visitors
Appendix 4: Glossary of Cyber Security Terminology
Appendix 5: School Social Media Guidelines for Staff

1. Context

The White House School is an independent specialist school for children and young people with additional and complex needs. We are part of Cavendish Education and are committed to transforming lives through highly personalised education, therapeutic support and ambitious teaching.

Our vision is **"Making Learning Possible Again."** We create a school where pupils feel safe, belong, achieve and thrive. Through removing barriers to learning, rebuilding confidence and fostering positive relationships, we empower every pupil to realise their potential and prepare for successful and fulfilling lives beyond school.

Our mission is to provide a nurturing, ambitious and mindful education that supports both academic progress and personal growth. Guided by our whole-school ethos of **Healthy Minds, Happy Hearts**, we create the conditions for every pupil to become **Ready to Learn and Prepared for Life**.

Everything we do is underpinned by our core values:

- **Ambition** – developing curiosity, courage and aspiration.
- **Resilience** – developing confidence, character and perseverance.
- **Community** – demonstrating kindness, integrity and respect.

We believe that pupils thrive when they feel safe, understood and valued. Our culture is built upon strong relationships, high expectations and a commitment to seeing the strengths and potential in every child. We are deeply nurturing without lowering expectations and remain unashamedly ambitious for every pupil.

Our practice is informed by the National Autistic Society's **SPELL Framework**, which promotes:

- Structure and predictability;
- Positive approaches and expectations;
- Empathy and understanding;
- Low arousal environments;
- Strong links between school, home and professionals.

Alongside this, we adopt a trauma-informed, relational and therapeutic approach across all aspects of school life. We recognise that behaviour is a form of communication and believe that pupils do well when they can. Our role is to understand the barriers they face and provide the support, strategies and relationships that enable them to succeed.

At The White House School:

- Every interaction is viewed as an intervention.
- Every adult is an emotionally available adult.
- Relationships come first.
- Emotional readiness is the foundation for learning.

We support pupils to develop emotional regulation, communication, independence and social understanding through consistent relational practice, personalised support and integrated therapeutic approaches. Emotional regulation is explicitly taught through co-regulation, sensory support, movement opportunities and personalised regulation strategies. Pupils are encouraged to understand themselves, develop resilience and build the skills needed to navigate life successfully.

Safeguarding is at the heart of everything we do. We recognise the additional vulnerabilities that many pupils with special educational needs may experience and maintain a culture of vigilance, care and advocacy. We place the child at the centre of decision-making, listen to pupil voice in all its forms and work closely with families and external agencies to promote safety, wellbeing and positive outcomes.

Through ambitious and adapted teaching, meaningful relationships, therapeutic support and a culture of belonging, we help pupils feel safe, build confidence, achieve success and thrive both in school and beyond.

2. Aims

This policy aims to:

- Ensure safe, responsible, and ethical use of school ICT resources by all users.
- Protect users and the school network from online risks and inappropriate content.
- Promote respect for intellectual property and data privacy.
- Set clear expectations for behaviour when using digital devices, internet, and communication tools.
- Support teaching, learning, and school operations through appropriate use of technology.
- Prevent misuse that could disrupt the school environment or compromise security.
- Encourage positive digital citizenship and awareness of online safety.

Breaches of this policy may be dealt with under our Staff Disciplinary policy, Positive Behaviour Support Policy and any other relevant policy.

3. Legislation and Guidance

This policy refers to, complies with, or otherwise has regard to, 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
- 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
- Meeting digital and technology standards in schools and colleges
- The Education (Independent School Standards) Regulations 2019
- Keeping children safe in education 2026 (comes into force from 1 September 2026)
- Working together to safeguard children 2026

4. Definitions

ICT facilities: all facilities, systems and services including, but not limited to, network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service that may become available in the future which is provided as part of the school's ICT service

Users: anyone authorised by the school to use the school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors

Personal use: any use or activity not directly related to the users' employment, study or purpose agreed by an authorised user

Authorised personnel: employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities

Materials: files and data created using the school's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

See appendix 5 for a glossary of cyber security terminology.

5. Unacceptable Use

The following is considered unacceptable use of the school's ICT facilities. Any breach of this policy may result in disciplinary or behaviour proceedings.

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing any web page or downloading any image, document, application, or file from the internet which could be regarded as illegal, offensive, discriminatory, in bad taste, or immoral
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community
- Using the school's systems to participate in internet chat rooms, post on internet message boards or blogs, unless approved by authorised personnel
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the school's ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the internet and network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to the school's ICT facilities
- Removing, deleting or disposing of the school's ICT equipment, systems, programmes or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school

- Using websites or mechanisms to bypass the school's filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way

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

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.

Sanctions

Pupils and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the school's policies on behaviour, discipline, staff discipline, staff code of conduct and safeguarding policies.

The school's policies are published and/or available on site or via the school's digital storage facilities that are available to all staff.

Misuse of ICT may result in the removal of access to ICT resources.

6. Staff

Access to school ICT facilities and materials
The school's ICT Manager manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

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

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

Staff who have access to files that they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the ICT Manager.

Use of Phones and Email
The school provides each member of staff with an email address. This email account should be used for work purposes only. All work-related business should be conducted using the email address the school has provided.

Staff must not share their personal email addresses with parents/carers or pupils and must not send any work-related materials using their personal email account. Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any external emails with attachments containing sensitive or confidential information must be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error that contains the personal information of another person, they must inform the ICT Manager and Data Protection Officer immediately and follow our data breach procedure.

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

School phones must not be used for personal matters.

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. The school can record incoming and outgoing phone conversations.

All non-standard recordings of phone conversations must be pre-approved and consent obtained from all parties involved.

If a conversation is likely to require specific recording for record keeping purposes this can done on a school device with audio recording features. This should be discussed in advance with the Headteacher. If this is going to happen then all of those involved in the call must be aware that it is being recorded. The reasons for doing so could include:

- Discussing a complaint raised by a parent/carer or member of the public
- Calling parents/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

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 ICT Manager, with approval, may withdraw or restrict this permission.

Personal use is permitted provided that such use:

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

Staff may not use the school's ICT facilities to store personal, non-work-related information or materials (such as music, videos or photos). Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the school's Staff code of conduct.

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where pupils and parents/carers could see them.

Staff should take care to follow the school's guidelines on use of social media (see school's social media Policy) and use of email (see section 5) to protect themselves online and avoid compromising their professional integrity.

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. Please refer to the school's Social Media policy as well as appendix 1 of this policy for guidelines on social media security settings.

Remote Access
The school allows staff to access the school's ICT facilities and materials remotely. Staff using the school's resources remotely must abide by the same rules as those accessing the facilities materials onsite. Staff should exercise caution with this and should be mindful that unauthorised downloading of material on to personal devices is not permitted. It should also be noted that all material on the school's ICT systems that has been generated, edited or otherwise created by a member of school staff is the intellectual property of the school. Unauthorised sharing of this could result in disciplinary or legal action against any individuals concerned.

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. If in any doubt the user must contact the school's Data Protection Officer.

School Social Media Accounts
The school has an official Facebook, Instagram and LinkedIn account, managed by the Headteacher. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account.

The school has guidelines for what may and must not be posted on its social media accounts. Those who are authorised to manage, or post to, the account must make sure they abide by these guidelines at all times. These can be found in appendix 6.

Monitoring and Filtering of the School Network and Use of ICT Facilities
To safeguard and promote the welfare of children and provide them with a safe environment to learn, the school reserves the right to filter and monitor the use of its ICT facilities and network. This includes, but is not limited to, the filtering and monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised ICT personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

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 School Board has ultimate responsibly 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. The Headteacher will oversee this compliance and monitor the performance of the Designated Safeguarding Lead.

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

7. Pupils

Pupils are provided with the following access to the school's ICT facilities:

- Laptop computers (either individually designated for use or shared machines)
- Tablets
- Desktop computers
- SMART boards

This access is permitted under supervision. Pupils are not provided with access to the school's wifi network other than when using the devices listed above.

Search and Deletion
Members of the Senior Leadership Team are authorised to lawfully search and delete from pupil's electronic devices.

Under the Education Act 2011, the Headteacher, and any member of staff authorised to do so by the school, can search pupils and confiscate their mobile phones, computers or other devices that the authorised staff member has reasonable grounds for suspecting:

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

This includes, but is not limited to:

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

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

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

- 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, however if co-operation is not given then the search can proceed and Positive Behaviour policy will be followed

The authorised staff member should:

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

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

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

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

If inappropriate material is found on the device, it is up to Headteacher, or those authorised by 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.

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

- They reasonably suspect that its continued existence is likely to cause harm to any person, **and/or**
- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- **Not** copy, print, share, store or save the image
- Confiscate the device and report the incident to the DSL (or deputy) immediately, who will decide what to do next. The DSL will make the

decision in line with the DfE's latest guidance on searching, screening and confiscation and the UK Council for Internet Safety (UKCIS) et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy

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

Unacceptable Use of ICT and the Internet Outside of School

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

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

The full range of sanctions available to the school will be considered and a proportional response, as determined by the school, will be made.

8. Parents and Carers

Parents and carers do not routinely have access to the school's ICT facilities and resources. If parents or carers are granted access, for a specific purpose, they must abide by those guidelines and rules that are specified for staff use of the school ICT facilities.

Communicating With or About the School Online
We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online.
Parents and carers play a vital role in helping model this behaviour for their children, especially when communicating with the school or about the school online.

The school is always keen to have an open and candid dialogue with parents about any issues that arise. It should be noted that the school fully reserves the right to take legal action for any defamatory information that is communicated online about the school.

Significant or repeated defamatory, untrue or misrepresentative comments (as determined by the school) made online could be used as grounds to terminate a placement agreement. Reserving and/or exercising this right is fully compliant with the The Education (Independent School Standards) Regulations 2019.
Communicating with Parents and Carers about Pupil Activity

The school will ensure that parents and carers are made aware of any online activity that their children are being asked to carry out. When we ask pupils to use websites or engage in online activity, we will communicate the details of this to parents/carers in the same way that information about homework tasks is shared.

In particular, staff will let parents/carers know which (if any) person or people from the school pupils will be interacting with online, including the purpose of the interaction. Parents/carers may seek any support and advice from the school to ensure a safe online environment is established for their child.

9. 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 cybercrime technologies.

Staff, pupils, parents/carers and others who use the school's ICT facilities should use safe computing practices at all times. We aim to meet the cyber security standards recommended by the Department for Education's guidance on digital and technology standards in schools and colleges, including the use of:

- Firewalls

- Security features
- User authentication and multi-factor authentication
- Anti-malware software

Passwords
All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure. The requirements for a secure password are embedded in the password changing process and cannot be circumvented by users.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control. Members of staff or pupils who disclose account or password information may face disciplinary action. Parents, visitors or volunteers who disclose account or password information may have their access rights revoked.

Staff are prompted and required to change their passwords every 30 days.

Software Updates, Firewalls and Anti-Virus Software
All of the school's ICT devices that support software updates, security updates and anti-virus products will have these installed, and be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.

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

Data Protection
All personal data must be processed and stored in line with data protection regulations and the school's data protection policy.

Access to Facilities and Materials
All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices.

These access rights are managed by the ICT manager.

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 ICT Manager immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. This applies any time when a user walks away from a piece of ICT equipment they are using. Equipment and systems should always be logged out of and shut down completely at the end of each working day.

Encryption

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

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

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

10. Protection from Cyber Attacks

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

- Work with Board Members and the IT department to make sure cyber security is given the time and resources it needs to make the school secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security, including how to:
- Check the sender address in an email
- Respond to a request for bank details, personal information or login details
- Verify requests for payments or changes to information
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether our IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Put controls in place that are:
  - **Proportionate**: the school will verify this using a third-party audit (such as 360 degree safe or SWGFL) 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. These reviews will be done by, or overseen by the Headteacher. This may be delegated to the DSL, but effective compliance remains the responsibility of the Headteacher.
  - Back up critical data at least weekly if stored offline and store these backups on non-networked external encrypted storage
  - Delegate specific responsibility for maintaining the security of our management information system (MIS) to ICT Manager
  - Make sure staff:

- Enable multi-factor authentication where they can, on things like school email accounts
- Store passwords securely using a password manager
- Make sure ICT staff conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
- Have a firewall in place that is switched on
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and checking if they have the Cyber Essentials certification
- Develop, review and test an incident response plan with the IT department including, for example, how the school will communicate with everyone if communications go down, who will be contacted and when, and who will notify Action Fraud of the incident. This plan will be reviewed and tested every 6 months and after a significant event has occurred, using the NCSC's 'Exercise in a Box'

11. Internet Access

The school's wireless connection is secure. There is internet filtering in place and response key stroke logging responses monitoring software. This software will notify Senior Leadership and DSL of any potentially harmful or inappropriate internet access. Pupils are not permitted wifi access on personal devices.

Parents/Carers and Visitors

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

The headteacher will only grant authorisation if:

- Parents/carers are working with the school in an official capacity (e.g. as a volunteer)
- 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.

12. Monitoring Arrangements

This policy will be reviewed by the Headteacher and approved by Directors every three years in consultation with the school board.

13. Links to Other Policies

This policy should be read in conjunction with the following policies:

- Online Safety Policy
- Social Media Policy
- Safeguarding and Child Protection Policy
- Positive Behaviour Management Policy
- Data Protection Policy

Approval & Policy Review

This Policy has been reviewed and approved by:

Policy Approver(s)	Sarah Moorcroft – Executive Headteacher
Storage Location	Online
Effective Date	September 2026
Next Review Date	July 2029

Revision History

Version	Change	Author	Date of Change
1	Updated policy for new academic year	Elle Vinall	July 2025
2	Updated format to match Cavendish Policies.	Elle Vinall	September 2026

Appendix 1: Facebook and Social Media Cheat Sheet for Staff

DO NOT ACCEPT FRIENDS REQUESTS FROM PUPILS OR PARENTS ON SOCIAL MEDIA

10 Rules for school staff on Facebook or other social media platforms

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if you don't, make sure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be happy showing your pupils
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there
8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the Facebook app from your phone. The app recognises WiFi connections and makes friend suggestions based on who else uses the same WiFi connection (such as parents or pupils)

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this
- Remember that **some information is always public**: your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What to do if…

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll

have to notify senior leadership and/or their parents/carers. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the headteacher about what's happening

A parent/carer adds you on social media

It is not appropriate to accept a friend request from a parent or carer from the school. Consult the school's Social Media policy of Staff code of conduct for more information.

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member notify the Headteacher immediately and the school can provide support, including through the school's behaviour and exclusions policy
- 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 Pupils and Parents/Carers

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS
Name of pupil:
Technology is an important part of learning at our school. This agreement explains how everyone can help keep themselves and others safe when using school technology. As a pupil, I agree that I will: **Use technology responsibly** ● Use school technology, devices, networks and online services safely, responsibly and respectfully. ● Use school technology for educational purposes unless a member of staff gives me permission to do otherwise. ● Follow my teacher's instructions when using computers, tablets, laptops, mobile devices or other digital technology. ● Respect other people when communicating or working online.
Keep myself and others safe ● Keep my usernames and passwords secure and never share them with anyone else. ● Protect my personal information and never share my full name, home address, telephone number, passwords or other personal details online without permission from a trusted adult. ● Tell a trusted adult immediately if: ○ I see anything online that worries, upsets or frightens me; ○ someone contacts me in a way that makes me feel uncomfortable; ○ I think another pupil may be at risk online; ○ I accidentally access inappropriate content; ○ I receive suspicious messages, emails or links.
Behave respectfully online I will: ● be kind and respectful to others; ● use appropriate language; ● respect other people's privacy; ● think carefully before posting or sharing anything online; ● understand that my online actions can have consequences. I will not: ● bully, threaten or deliberately upset anyone online; ● share embarrassing, offensive or harmful content; ● create or share fake accounts or impersonate another person; ● share photographs, videos or recordings of other people without permission.

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Use Artificial Intelligence (AI) responsibly

Where AI tools are authorised by the school, I will:

- use them only for learning purposes;
- follow my teacher's instructions;
- never use AI to bully, embarrass or harm another person;
- never create or share AI-generated images or videos that could upset or exploit someone;
- not submit AI-generated work as my own if this is against my teacher's instructions;
- remember that AI can sometimes provide incorrect or misleading information.

Use the internet safely

I will not:

- access inappropriate websites or material;
- deliberately try to bypass the school's filtering or monitoring systems;
- download software or files without permission;
- open unknown email attachments or click suspicious links;
- arrange to meet anyone I have met online without the knowledge and permission of my parent/carer.

Look after school equipment

I will:

- look after school devices and equipment;
- report damaged equipment immediately;
- log off or lock devices when I have finished using them;
- only use equipment that I have permission to use.

Mobile phones and personal devices

If I bring a mobile phone or personal device into school, I will:

- follow the school's Mobile Phone Policy;
- keep my device switched off or stored securely during the school day unless a member of staff gives permission to use it;
- not use my device to photograph, film or record anyone without permission;
- not use personal devices to access inappropriate content or communicate inappropriately.

Filtering and Monitoring

I understand that:

- the school uses filtering and monitoring systems to help keep everyone safe online;
- my activity on school devices and networks may be monitored;
- if I do not follow this agreement, appropriate action will be taken in line with the school's Behaviour Policy and Online Safety Policy.

I understand how to use technology safely and responsibly and will follow these expectations whenever I use school technology.

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Signed (pupil):	Date:
Parent/carer's agreement: **I understand that:** • technology is an important part of my child's education; • the school uses filtering and monitoring systems to help safeguard pupils; • my child is expected to use technology safely, responsibly and respectfully; • I will support the school's expectations for the safe use of technology at home and at school; • I will encourage my child to tell a trusted adult if they experience anything online that worries or upsets them; • I will work with the school if an online safety concern arises; • I understand that misuse of school technology or breaches of this agreement may result in appropriate safeguarding or disciplinary action. • I have discussed this agreement with my child and will support them in following these expectations.	
Signed (parent/carer):	Date:

Appendix 3: Acceptable Use of the Internet - Agreement for Staff and Visitors

Acceptable Use Agreement (Staff)

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital technologies are powerful tools which open up new opportunities for everyone. These technologies can stimulate discussion and promote creativity, promoting effective learning. They also bring opportunities for staff to be more creative and productive in their work.

This Acceptable Use Agreement is intended to ensure:

- that staff and volunteers will be safe and responsible users of the internet and other digital technologies.
- that school ICT systems and users are protected from accidental or deliberate misuse.

The school will try to ensure that staff and volunteers have good access to ICT to enhance their work and improve opportunities for learners, and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Agreement

I understand that I must use school ICT systems in a responsible way, to minimise the risk to my safety or to the safety and security of the ICT systems and other users. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of its ICT systems, including email and other digital communications technologies. This may include, but not be limited to, the following circumstances:
    - With software to monitor 'trigger' words or phrases for safeguarding and to ensure acceptable, professional use of IT.
    - When staff leave or are on long-term absence, for the retrieval or redirection of messages.
    - When a member of staff is under investigation or suspected of illegal, fraudulent, inappropriate or safeguarding activity.
    - To collect and review information contained in any electronic system for documented purposes and authorised by [insert name of appropriate member of staff], for example, to complete a Subject Access Request or similar.
- I understand that information and resources stored on the organisation's equipment and drives should be considered to be controlled and accessible by the School and authorised staff.
- I understand that this agreement also applies to the use of school ICT systems out of school (eg laptops, email, VLE, etc). This includes my personal or work mobile phone or tablet if it contains my work email.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will keep my usernames and passwords private and will not try to use anyone else's username and password.

- I will not share or continue to use any logins for any school service or platform when I leave my employment.
- I will return all school-owned ICT equipment and delete all school data from my personal devices when I leave my employment.

- I will immediately report any illegal, inappropriate or harmful material or incident to the Head Teacher or other person appointed by the Head Teacher/DPO

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, delete or otherwise alter any other user's files without their permission.
- I will communicate with others in a professional manner.
- I will ensure that when I take or publish images of pupils or parents/colleagues, I will do so with their permission and in accordance with the school's Agreement. I will not use my personal equipment to record these images unless I have permission to do so.
- Where these images are published (eg on the school website / VLE) it will not be possible to identify pupils by name or other personal information.
- I will not use chat and social networking sites in school.
- I will only communicate with pupils and parents/carers using official school systems and in a professional manner. I will not share any personal information with a pupil (including personal phone numbers or email addresses). Nor will I request or respond to any personal information from a young person unless it is appropriate as part of my professional role.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will lock my screen or log off my computer should I leave it unattended.
- I will not allow a third party to access my work emails on my mobile phone or tablet

The school and the local authority have the responsibility to provide safe and secure access to technologies:

- When I use my personal handheld/external devices in school (PDAs / laptops / mobile phones / USB devices, etc), I will follow the rules set out in this agreement, in the same way as if I were using school equipment. I will also follow any additional rules set by the school about such use. As far as I am able, I will ensure that when connecting these devices to school ICT systems, they are using up-to-date Operating Systems (e.g. latest versions of Android / iOS) and protected by up-to-date anti-virus software where applicable.
- I will not save any personal data on my personal computer.
- I will not use my personal WhatsApp accounts to share organisational data, such as student data, staff information, or any other confidential school-related details.
- I will only use the recommended apps on my personal device for accessing data\emails via Office 365 or G-Suite.
- I will encrypt (Password Protect in most cases) my personal device if I use it to access school personal data or Office 365\G-Suite apps.
- I will inform the school's Head Teacher or other person appointed by the Head Teacher/DPO if my personal device, e.g. phone or tablet, is lost or stolen, should it contain any school personal data.
- I will immediately report any Internet content that is not filtered that I suspect could be inappropriate.
- I will delete personal data according to the school's retention policy.
- I will not use personal email addresses for work-related purposes.

1

- I will not open any attachments to emails unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programs.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.

- I will not upload, download or access any material which is illegal or inappropriate or may cause harm or distress to others (eg child sexual abuse images, criminally racist material, adult pornography, etc).
- I will not use any programmes or software that might allow me to bypass the filtering/security systems intended to prevent access to such materials.
- I will not install or attempt to install programmes of any type on school systems, nor will I alter computer settings, unless this has been authorised.
- I will not disable or cause any damage to school equipment or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Protection Policy. Where personal data is electronically transferred outside the secure school network, it must be encrypted.
- I will immediately report any damage or faults involving equipment or software; however, this may have happened.

When using the internet in my professional capacity or for school-sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

System Specific Guidelines & Procedures
Use of Electronic Whiteboards and Screensharing

- I understand that electronic whiteboards should be used in a manner that upholds the school's standards of professionalism and respect.
- I will ensure that any content displayed or written on electronic whiteboards during lessons or meetings is appropriate for the intended audience.
- I will not save or store sensitive information displayed on the whiteboard without the necessary permissions or safeguards in place.
- When using interactive features, I will ensure that student data and privacy are protected at all times.
- When sharing the screen of my device (laptop, tablet, work phone etc) to the electronic whiteboard, I will ensure that only the necessary applications or windows are visible to avoid unintentionally sharing sensitive or personal information. This also applies to screensharing during online remote lessons or meetings.
- I will be vigilant and ensure that any notifications or pop-ups that may contain personal or sensitive information are disabled before sharing my screen to the electronic whiteboard. This also applies to screensharing during online remote lessons or meetings.
- I will ensure that any shared content displayed on the electronic whiteboard or shared during online remote lessons or meetings upholds the school's standards of professionalism and respect.

School's Management Information System (MIS)

- I understand that the school's MIS contains sensitive data and information pertinent to the functioning of the school.
- I will only access the MIS with the appropriate permissions and for legitimate school-related purposes.

- I will not share my MIS login credentials with anyone and will ensure that I log out after each session.
- I will ensure that I do not display or share information from the MIS with individuals who are not authorised the access the data (for example, by displaying the MIS on classroom screens or electronic whiteboards).
- I will immediately report any suspected breaches or unauthorised access to the MIS to the school's IT department.
- I will use multi-factor authentication, where available, to enhance the security of my access to the MIS.

School's Safeguarding System (MyConcern)

- I acknowledge the sensitive nature of data within the school's safeguarding systems and will handle this information with utmost care and discretion.
- I will ensure that I only access these systems for legitimate safeguarding-related activities and will avoid unnecessary browsing or querying of data.
- I will not share my login credentials for safeguarding systems with anyone.
- I will ensure that I do not display or share information from the Safeguarding System with individuals who are not authorised the access the data (for example, by displaying the MIS on classroom screens or electronic whiteboards).
- Multi-factor authentication should be used when accessing these systems to ensure the highest level of security.
- Any suspected breaches, mishandling, or unauthorised access to these systems should be reported immediately to the designated safeguarding lead.

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Agreement applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action and, in the event of illegal activities, the involvement of the police.

I have read and understand the above and agree to use the school ICT systems both in and out of school and my own devices (in school and when carrying out communications related to the school) within these guidelines.

School	
Print Name	
Date	
Signed	

3

Appendix 4: 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. Many of these terms are 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.

Appendix 5: School Social Media Guidelines for Staff

Social Media Use

Staff are reminded of their safeguarding statutory duties outline in KCSIE. Staff need to ensure that their use of social media must also be acceptable and not blur personal and professional boundaries or leave your professional conduct in question. Staff are not permitted to contact parents outside of school hours, nor on personal devices as this can leave them vulnerable and also blurs professional boundaries. It is accepted however that some staff may have existing relationships with parents of pupils who subsequently attend the school. In this instance professional judgement must be exercised. The school must not be brought into disrepute at any time and the confidentiality of all staff and pupil information must always be maintained.

On any social media platform, but especially Facebook, it is wise to check your privacy settings regularly and refer to the following advice:

- Change your display name so you are not easily identifiable.
- Change your profile picture to something unidentifiable, or if not, ensure that the image is professional.
- Be careful about tagging other staff members in images or posts
- Do not share anything publicly that you wouldn't be happy if your line manager, parents or pupils can see.
- Do not use social media sites during school hours
- Do not make comments about your job, your colleagues, our school or our pupils online.
- Do not associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
- Do not link your work email address to your social media accounts.

You can check your privacy settings on Facebook using the following advice and guidance:

- 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 have 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: https://www.facebook.com/help/236898969688346/?helpref=uf_share to find out how to limit the visibility of previous posts
- 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

Under no circumstances should you accept a 'friend request' from a pupil. If you are contacted online by a pupil, please refer this matter at your earliest opportunity to a member of the Safeguarding team.

It would not be permissible to accept a 'friend request' from a parent of a pupil. This may leave you vulnerable and certainly blurs professional and personal boundaries. It is accepted that existing relationships with parents of pupils who subsequently attend the school may mean existing online connections. However, the staff member is responsible at all times for their conduct and should be mindful of professional expectations as well as those relating to the teacher or HLTA standards.
If you need any help with online safety or have any concerns about harassment or abuse, you can speak to our Online Safety Champion or any member of the Safeguarding Team. You may also find the following information useful:

- Do not retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent 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

Gaming
It should be noted that all rules relating to social media use and contact with pupils also applies to online gaming. It would never be acceptable to game against a pupil of the school online, or to communicate with them through such platforms. This blurs professional boundaries and is always inappropriate. In the event a member of staff unexpectedly finds themselves in contact with a pupil online in this way, it must immediately end and the Headteacher should be informed of it at the next appropriate opportunity. All efforts should then be made by the member of staff to block the young person from making further contact via the aforementioned means.