DOWNLANDS
COMMUNITY SCHOOL

Digital Systems Policy

Approved by:	Full Governing Board	**Date**: 24 January 2024
Last reviewed by: **on:**	C. Davies, M. Lincoln January 2024	
Next review due by:	January 2026 – *this policy is currently under review.*	

This policy should be read in conjunction with the School Data Protection Policy and Abusive Parents/Carers Policy

1 AIM

To promote learning using technology and provide guidelines for its use.

2 POLICY CONTENTS

CONTENTS

3 RELEVANT LEGISLATION AND GUIDANCE

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

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- Education and Inspections Act 2006
- Keeping Children Safe in Education 2023
- Searching, screening and confiscation: advice for schools 2022
- National Cyber Security Centre (NCSC): Cyber Security for Schools
- Education and Training (Welfare of Children) Act 2021
- UKCIS 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

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

- Discipline and Student Behaviour
- GDPR Staff Guidance
- GDPR
- Safeguarding
- Staff Disciplinary

4 CONDITIONS OF USE

4.1 PERSONAL RESPONSIBILITY:

Access to Downlands Community School's networked resources is a privilege, not a right. Users are responsible for their behaviour and communications. Staff and pupils will be expected to use the resources for the purposes for which they are made available. Users are to take due care with the physical security of hardware they are using. Users will accept personal responsibility for reporting any misuse of the network to the Systems Manager.

It is the responsibility of the User (where appropriate) to take all reasonable steps to ensure compliance with the conditions set out in this Policy document, and to ensure that unacceptable use of the Internet/Intranet does not occur.

Staff or students finding unsuitable websites through the school network should report the web address to the IT Technicians.

4.2 ACCEPTABLE USE:

Users are expected to utilise the network systems in a responsible manner. Unacceptable use of the network or systems may result in disciplinary or behaviour proceedings.

4.2.1 Network Etiquette:

1. Be polite – never send or encourage others to send abusive messages.
2. Use appropriate language – users should remember that they are representatives of the school on a global public system.
3. Do not attempt to visit websites that might be considered inappropriate (including those relating to illegal activity). All sites visited leave evidence in the county network if not on the computer.
4. Make sure your passwords are secure. If you think someone has learned your password, then contact the IT Technicians.
5. Log off after your session has finished.
6. Users finding machines logged on as another user should log off the machine whether they intend to use it or not.
7. Electronic mail is not guaranteed to be private and may be searched when needed.
8. Users may only store relevant work on the system, users found to have large numbers of pictures or music will have them deleted and will be sanctioned appropriately.

4.3 UNACCEPTABLE USE

Below details examples of Unacceptable Use. This, however, is not an exhaustive list and the school reserves the right to amend this list at any time. The Senior Leadership Team, with advice from the IT technicians and relevant authorities, will use their professional judgement to determine whether any act or behaviour not on the list is considered unacceptable use of the school's ICT facilities.

4.3.1 Unacceptable Language and Behaviour:

1. Use of language that is discriminatory or could be calculated to incite hatred against any protected characteristic group.
2. Bullying or harassing others.
3. Attempting to access or use of unsupervised and/or unauthorised chat rooms.
4. Activity which defames or disparages the school, or risks bringing the school into disrepute.
5. Promoting a private business, unless that business is directly related to the school.

4.3.2 Unacceptable use of ICT facilities for illegal activities:

Illegal activities of any kind are strictly forbidden. Any suspected illegal activities may be reported to and investigated by relevant authorities.

1. Engaging in content or conduct that is radicalised, extremist, racist, antisemitic, or discriminatory in any other way.
2. Statements or e-mails relating to or in support of illegal activities.
3. Breaching intellectual property rights or copyright.
4. Downloading illegal material. This will be referred to the police or other authorities to investigate as appropriate.
5. Online gambling, inappropriate advertising, phishing and/or financial scams.
6. Accessing, creating, storing, linking to, or sending material that is pornographic, offensive, obscene, or otherwise inappropriate or harmful.
7. Sharing consensual or non-consensual nude and semi-nude images and/or videos and/or livestreams.

4.3.3 Unacceptable Use related to Privacy:

1. Revealing any personal information (e.g., home address, telephone number) about yourself or other users online.
2. Trespassing into other users' files or folders.
3. Sharing confidential information about the school, its pupils, or other members of the school community.

4.3.4 Unacceptable Use of Equipment and Network:

1. Using the network in any way that would disrupt use of the network by others.
2. Introducing any device, USB drive or memory card into the network. All devices must be processed by the school IT technicians.
3. Unapproved system utilities and executable files stored on the system or attached to e-mail. Files held on the school's network may be regularly checked by the IT Technicians to monitor this.
4. Causing intentional damage to the school's ICT facilities.
5. Downloading or installing any software, applications, or web services on the school's network without approval by the IT technicians.
6. 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.
7. Gaining, or attempting to gain, access to restricted areas of the network, or any password-protected information. Please refer to the IT technicians if you think you should have access.

8. Allowing, encouraging, or enabling others to gain, or attempt to gain, access to the school's ICT facilities.
9. Accessing, modifying, or sharing data (including personal data) which the user or recipient should not have access to. This is a Data Breach and must be reported to the Data Manager and IT Technician even if accidental.
10. Removing, deleting, or disposing of ICT equipment, systems, programmes, and information without authorisation from the IT technicians.
11. Sharing a Wi-Fi password or private Pre-Shared Key (PPSK).

4.4 Monitoring and Filtering

1. 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
    - User activity/access logs
    - Any other electronic communications
2. The school monitors ICT use to:
    - Safeguard students and staff
    - 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
3. Only authorised ICT personnel may filter, inspect, monitor, intercept, assess, record, and disclose the above, to the extent permitted by law.
4. The entire network is monitored by Securis at all times.
5. Internet traffic is monitored and filtered by Schools Broadband.
    - Schools Broadband supports full compliance with the following requirements: Prevent Duty Keeping Children Safe in Education Internet Watch Foundation (IWF) Block List and Image Hash List Home Office Terrorism Block List UK Safer Internet Centre.
    - Schools Broadband's Appropriate Filtering Response can be found at https://www.schoolsbroadband.co.uk/wp-content/uploads/Appropriate-Filtering-Provider-Response-2023.pdf.
6. Net Support is used by IT technicians to remote access PCs around the school.
7. Personal devices linked to the school network have an individual private Pre-Shared Key (PPSK) that cannot be shared.
8. Where appropriate, authorised personnel may raise concerns about monitored activity with the school's Designated Safeguarding Lead (DSL) and Systems Manager, as appropriate.

9. The effectiveness of any filtering and monitoring will be regularly reviewed by the Systems Manager and schools governing body.

5 SOCIAL MEDIA

5.1 CONTEXT

Social media (e.g., Facebook, Instagram, LinkedIn) is a broad term for any kind of online platform which enables people to directly interact with each other. Additionally, some games (e.g., Minecraft) and video sharing platforms (e.g., You Tube) have social media elements to them.

1. The school recognises the numerous benefits and opportunities which a social media presence offers.
2. Staff, parents/carers, and pupils/students are encouraged to find creative ways to use social media. However, there are some risks associated with social media use, especially linked to safeguarding, bullying and personal reputation.
3. Professional communications are those made through official channels, posted on a school account, or using the school name. All professional communications are within the scope of this policy.
4. The school respects privacy and understands that staff and pupils/students may use social media in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.
5. Personal communications made via a personal social media account which do not refer to or impact upon the school are outside the scope of this policy.
6. Staff may use official School Social Media accounts to communicate with learners for teaching and learning purposes but must consider whether this is appropriate and consider the potential implications.
7. The Senior Leadership Team will take a lead role in investigating any reported incidents including an initial assessment and contacting relevant staff or external agencies.

5.2 LEGAL CONSIDERATIONS

1. Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.
2. Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.
3. Unacceptable conduct, (e.g., defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered seriously by the school and will be reported as soon as possible to a senior member of staff and escalated where appropriate.
4. The school will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies and may take action according to the disciplinary policy.

5.3 Monitoring posts about the school

1. As part of active social media engagement, it is considered good practice to pro-actively monitor the internet for public postings about the school.
2. Any posts requiring attention or reply should be directed to the Senior Leadership Team.
3. SLT will draft responses to social media posts with advice from external parties where necessary.
4. Offensive or unacceptable posts will be reported to the social media platform and those users may be blocked.

5.4 Use of images

1. The school may use images of students and staff online and on its official social media accounts in strict accordance with our GDPR Policy.
2. We will obtain consent from parents/carers for photographs and videos to be taken of pupils for communication, marketing, and promotional materials.
3. Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.
4. Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Students should be appropriately dressed, not be subject to ridicule.
5. Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we do ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons.
6. Students and parents/carers should not publicly post images of staff on social media accounts without consent.

For further details please see the GDPR Policy.

6 Staff (including governors, Trainees, and Agency Employees)

6.1 Access to school ICT facilities and materials

1. The school's Systems Manager manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:
    a. Computers, tablets, mobile phones, and other devices
    b. Access permissions for certain programmes or files
2. Staff will be provided with unique login/account information and passwords that they must use when accessing the school's ICT facilities.
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 the IT technicians.
4. 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.

6.2 USE OF PHONES AND EMAIL

1. The school provides each member of staff with an email address. This email account should be used for work purposes only.
2. All work-related business should be conducted using the email address the school has provided.
3. Staff must not share their personal email addresses with parents or pupils and must not send any work-related materials using their personal email account.
4. 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. 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.
6. 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.
7. 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.
8. If staff send an email in error that contains the personal information of another person, they must inform the Data Manager immediately who will action our data breach procedure.
9. Staff must not give their personal phone number(s) to parents or pupils. Staff must use phones provided by the school to conduct all work-related business.
10. School phones must not be used for personal matters.
11. 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.

6.3 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 Systems Manager may withdraw or restrict this permission at any time and at the discretion of SLT.

1. Personal use is permitted provided that such use:
    a. Does not take place during contact time.
    b. Does not constitute 'unacceptable use', as defined in section 4.
    c. Takes place when no pupils are present.
    d. Does not interfere with their jobs or prevent other staff or pupils from using the facilities for work or educational purposes.
2. Staff should be aware that use of the school's ICT facilities for personal use (including storing personal or non-work related materials) may put anything stored within the scope of the school's ICT monitoring activities[1]. Where breaches of this policy are found, disciplinary action may be taken.

[1] See section 4.4.

3. Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with 4. Conditions of Use. Personal devices have limited access to the school network and internet.
4. 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 could see them.
5. Staff should take care to follow the school's guidelines on use of social media[2] and use of email[3] to protect themselves online and avoid compromising their professional integrity.

6.4 Remote Access

We allow staff to access the school's ICT facilities and materials remotely. This includes Cloud Based access such as Microsoft 365 or Bromcom, as well as remotely accessing the server.

1. 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.
2. Staff must be particularly vigilant outside the school and take recommended precautions against compromising system security in addition to preserving the confidentiality of staff and student data.

Staff may access the sever remotely using Microsoft's Remote Desktop software. It is managed by the IT technicians who also audit usage and keep logs. Instructions on how to use the remote desktop software can be requested from it@downlands.org or found on the staff network.

6.5 Social Media

In addition to the guidance stated in Section 5: Social Media, staff should also adhere to the below points.

6.5.1 Behaviour

1. Unacceptable conduct, (e.g., defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered seriously by the school and will be reported as soon as possible to a senior member of staff and escalated where appropriate.
2. The school will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies and may take action according to the disciplinary policy.
3. Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff.
4. If a conversation turns and becomes offensive or unacceptable, school users should block, report, or delete other users or their comments/posts and should inform the audience exactly why the action was taken.
5. If you feel that you or someone else is subject to abuse by colleagues through use of a social media platform, then this action must be reported to SLT and/or the HR Officer.

[2] See section 6.5.
[3] See section 6.2.

6. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school.

6.5.2 Personal social media accounts

1. Personal communications are those made via a personal social media account.
2. Where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are subject to monitoring by the school.
3. Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
4. Staff are not permitted to follow or engage[4] with current or prior students (up to the age of 19) of the school on any social media platforms.
5. Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.
6. Staff should never post images of current or prior students on their personal social media accounts.
7. Further advice and guidelines on personal use of social media can be found in appendix 2 and on the ICT Training Site.

6.5.3 School social media accounts

The school has official Facebook, Twitter, and Instagram accounts, run by the Social Media Manager, and managed by SLT.

1. Staff members who have not been authorised to manage, or post to, official school accounts, must not access, or attempt to access, the account.
2. Department specific accounts must be set up with permission from SLT and information given to the Social Media Manager.
3. Use of images in social media posts should strictly follow guidelines[5] and the schools GDPR policy. Under no circumstances should staff share or upload student pictures online other than via school owned social media accounts.
4. Staff should regularly monitor and manage content posted on professional accounts they run.
5. Account details, including passwords must be stored securely and passed on or changed when a staff member managing the account leaves.
6. Digital communications by staff must be professional and respectful at all times and in accordance with this policy.
7. School social media accounts must not be used for personal gain.
8. Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to school activity.
9. If a journalist makes contact about posts made using social media, staff must contact SLT immediately before responding.

[4] Engagement entails responding to public or private posts, messaging, tagging, or including a student in a post. This definition may differ across different platforms and may change over time.

[5] See section 5.4.

10. Comment, queries, or complaints should be promptly reported to SLT for advice on responding with sensitivity.

7 PUPILS

7.1 ACCESS TO ICT FACILITIES

1. Computers and equipment in the school is available to pupils only under the supervision of staff.
2. Specialist ICT equipment, such as that used for music, or design and technology, must only be used under the supervision of staff.
3. Pupils are provided with an account for the school network which they can access in school, as well as accounts for Office 365 and Bromcom which they can access both in school and on personal devices.
4. Students are required to sign the Acceptable Use policy before being allowed access to the school's ICT facilities.
6. Students are also permitted to use their personal devices (such as mobile phones or tablets) in line with Section 4: Conditions of Use, and Appendix 3: Use of Student-Owned Internet Enabled Devices in School
7. Personal devices have limited access to the school network and internet.

7.2 INTERNET ACCESS

1. Pupils are given access to the internet through school-maintained devices and may request to join their personal device to the student Wi-Fi network with permission from a parent or carer.
2. Security and filtering is as stated in monitoring and filtering [6].
3. All personal devices are given an individual private Pre-Shared Key (PPSK) so that Wi-Fi passwords may not be shared between devices.
4. Once a parent or guardian has given a permission (on MCAS or paper), a pupil may go to the IT technicians and ask for them to add their device to the Wi-Fi network.
5. The "curriculum" network has limited access to school data and a stricter internet filtering system, including a ban on social media websites, and known gaming websites.

7.3 SEARCH AND DELETION

Under the Education Act 2011, the headteacher, and any member of staff authorised to do so by the headteacher, can search pupils and confiscate their mobile phones, computers, or other devices. Further details of this can be found in the Discipline and Student Behaviour Policy.

7.4 UNACCEPTABLE USE OF ICT AND THE INTERNET OUTSIDE OF SCHOOL

The school may sanction pupils and/or contact the authorities, in line with the Discipline and Student Behaviour Policy, if a pupil engages in any of the following at any time (even if they are not on school premises):

[6] See section 4.4.

1. Using ICT or the internet to breach intellectual property rights or copyright.
2. Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination.
3. Breaching the school's policies or procedures
4. Any illegal conduct or making statements which are deemed to be advocating illegal activity.
5. Accessing, creating, storing, linking to, or sending material that is pornographic, offensive, obscene, or otherwise inappropriate.
6. 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)
7. Activity which defames or disparages the school, or risks bringing the school into disrepute.
8. Sharing confidential information about the school, other pupils, or other members of the school community
9. Gaining or attempting to gain access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel.
10. Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities.
11. Causing intentional damage to the school's ICT facilities or materials
12. 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.
13. Using inappropriate or offensive language
14. Further guidance for using Social Media can be found in appendix 2.

8 PARENTS/CARERS

8.1 ACCESS TO ICT FACILITIES AND MATERIALS

Parents do not have access to the school's ICT facilities as a matter of course.

However, parents working for, or with, the school in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access or be permitted to use the school's facilities at the headteacher's discretion.

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

8.2 COMMUNICATING WITH OR ABOUT THE SCHOOL ONLINE

1. We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online.
2. Parents 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.
3. We ask parents to co-sign the Acceptable Use Policy agreement on admission.
4. Parents/Carers are encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person in accordance with the Complaints Procedure policy.

8.3 COMMUNICATING WITH PARENTS ABOUT PUPIL ACTIVITY

1. Staff will let parents know if pupils will be interacting with online with any persons outside the schools, including the purpose of the interaction. For example a pen pal exchange with students from another school.
2. Parents 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 cyber-crime technologies.

Staff, pupils, parents, and others who use the school's ICT facilities should always use safe computing practices. 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
- Anti-malware software

9.1 PASSWORDS

1. All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure. If you think someone has learned your password, contact the IT Technicians.
2. Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.
3. Members of staff or pupils who disclose account or password information may face disciplinary action. Parents/Carers, visitors or volunteers who disclose account or password information may have their access rights revoked.

9.2 SOFTWARE UPDATES, FIREWALLS AND ANTI-VIRUS SOFTWARE

1. All 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.
2. 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.

9.3 DATA PROTECTION

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

9.4 Access to facilities and materials

1. All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices which are managed by the Systems Manager.
2. Users should not access, or attempt to access, systems, files, or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the IT Technicians immediately.
3. Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and shut down completely at the end of each working day.

9.5 Encryption

1. The school makes sure that its devices and systems have an appropriate level of encryption.
2. School staff may only take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the headteacher.
3. Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the Systems Manager.

10 Protection from cyber attacks

The school will:

1. Work with governors and the IT department to make sure cyber security is given the time and resources it needs to make the school secure.
2. Make sure staff are aware of its procedures for reporting and responding to cyber security incidents.
3. Investigate whether our IT software needs updating or replacing to be more secure.
4. Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data.
5. Put controls in place that are:
    a. Proportionate: the school will verify this through audits to test efficacy
    b. Multi-layered: everyone will be clear on what to look out for to keep our systems safe
    c. Up to date: with a system in place to monitor when the school needs to update its software.
    d. Regularly reviewed and tested: to make sure the systems are as effective and secure as they can be.
6. Create daily, weekly, monthly, and annual backups of critical data on backup tapes and maintain copies stored off the school premises overnight. Manage Barracuda to back up cloud-based data from Microsoft 365.
7. Delegate specific responsibility for maintaining the security of our Management Information System (MIS) to Bromcom.
8. Make sure staff enable multi-factor authentication where they can, on things like school email accounts.

9. 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.
10. Have a firewall in place that is switched on.
11. 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.
12. Work with our Local Authority to see what it can offer the school regarding cyber security, such as advice on which service providers to use or assistance with procurement.

Please see Appendix 4 for a Glossary including cyber security terminology.

11 Internet access

The school's wireless internet connection is secure.

1. Wi-Fi and Ethernet is provided throughout the school and is managed and maintained by the IT technicians. Filtering is provided as part of the internet provider, Schools Broadband and any inappropriate sites are flagged by the ICT monitoring system and communicated directly to Schools Broadband.
2. There are separate connections for Staff, Students, and Visitors with different levels of access.
3. Visitors who are authorised to have access will be given a temporary private Pre-Shared Key (PPSK) which gives limited access to the network and internet and expires after a set time. Where visitors are granted access, they must abide by this policy as it applies to staff.

12 Monitoring and review

The Headteacher and Senior Leadership Team monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every 1 years.

The governing board is responsible for reviewing/approving this policy.

13 Appendices

13.1 Appendix 1: Remote Learning Acceptable Use

13.1.1 Staff must:

- Use the platform Microsoft Teams.
- Record the lesson.
- Ensure only school staff and students appear/are heard on screen.
- Adhere to professional school guidelines.
- Follow the school dress codes.
- Use an appropriate background.
- Block and report any unacceptable use by students.

- Contact students only through the platforms agreed by the school and not through personalised accounts open to public viewing, comments or sharing.
- Teach content that is age appropriate and in line with the curriculum schemes that are in place - including retrieval and some phased new knowledge.
- Be clear, when using links to other online resources, that these resources are appropriate in nature and relevant to the learning process.

13.1.2 Students must:

- Follow the network etiquette above. In remote learning circumstances sharing passwords with parents/guardians is permitted.
- Use appropriate language and not make derogatory verbal or written comments about other participants in the lesson – this could be perceived as online bullying.
- Not record or take photos of peers or teachers during live lessons, nor share lessons publicly.
- Only use technology at home with the permission of their parent / guardian.
- Start the lesson with their cameras off and their audio muted. Teachers may ask students to use their camera or audio later in the lesson.
- Conduct video learning in an open space at home using a table or desk and chair.
- Be dressed appropriately for learning in home clothes (e.g., no pyjamas, no vest tops, hats, or hoods etc.).
- Not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If a student accidentally comes across any such material, they should report it immediately to their teacher or parent/guardian.
- Be attentive in lessons and not use personal social media in lesson time.

Students will be removed from lessons, and parents contacted, if their online conduct is inappropriate. Teachers can see everything students type and are recording the lesson. Audio, video, or screenshots from the lesson will be used if a student has behaved inappropriately.

13.2 Appendix 2: Social Media Cheat Sheet

1. Nothing on social media is truly private.
2. Social media can blur the lines between your professional and private life. Don't use the school logo and/or branding on personal accounts.
3. Check your settings regularly and test your privacy.
4. Keep an eye on your digital footprint.
5. Keep your personal information private.
6. Regularly review your connections – keep them to those you want to be connected to
7. When posting online consider; Scale, Audience and Permanency of what you post.
8. If you want to criticise, do it politely.
9. Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
10. Know how to report a problem.
11. The public may still be able to see posts you've interacted with, even if your profile settings are private, because this depends on the privacy settings of the original poster.
12. Google your name to see what information about you is visible to the public.
13. Remember that some information is always public: your display name, profile picture.
14. What to do if you're being harassed on social media
    a. Do not retaliate or respond in any way.
    b. Save evidence of any abuse by taking screenshots and recording the time and date it occurred.
    c. Report the material to Facebook or the relevant social network and ask them to remove it.
    d. If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents.
    e. 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.
    f. 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.

13.3 Appendix 3: Use of Student-Owned Internet Enabled Devices in School

At Downlands we regularly review the latest developments in technology with a view to utilising them to enhance the quality of teaching and learning.

We have made considerable investment in a state of the art site-wide wireless system (Wi-Fi). This opens up new possibilities for the use of technology in all lessons. We are investing in mobile devices for use by students across the curriculum. We are aware, however, that students increasingly have internet-enabled mobile devices that they may wish to use on permitted occasions in lessons.

Before we authorise the use of student devices, the terms and conditions listed below must be agreed to by their parent or carer. Please consider these carefully before giving your permission by signing and returning the attached slip.

The terms and conditions apply to all mobile internet enabled devices, comprising of, but not exclusively: iPads, iPods, laptops, smartphones or tablets.

If you wish your child to be able to access the internet using their own devices in school lessons (at the teacher's discretion), then you will need to give your consent, on the understanding that:

- The school does not take any responsibility for the loss or damage of any student-owned device. Students will be responsible for the safety of their devices in school and when travelling to and from school.
- There will be no facility in school for students to charge their devices. They are responsible for ensuring that any device is fully charged for use.
- Access to the Wi-Fi is conditional on all users agreeing to abide by the AUP (Acceptable Use Policy). All students will have signed an AUP form upon entry to the school. This emphasises what is 'acceptable use of the school's computer network' and highlights what is NOT acceptable. A copy is available on the school website in the 'Schools Policies' section of the 'About' tab.
- This does not change the school's current policy on the use of mobile phones for messaging or calling, which states that their use is forbidden at any time on the school site.
- Lessons where the use of students' mobile devices is permitted will be agreed in advance by the teacher and communicated clearly to the pupils. Students must not assume that the use of mobile devices is permitted in every lesson.

Every device will need to be registered with our technical team prior to use.

Any infringement of the AUP may result in access to the all of the school computer networks being withdrawn.

This policy will be reviewed and could be withdrawn or amended in the future.

If you wish your child to be authorised to use mobile devices in school for the purposes of accessing the internet, please complete and return the required form. Students will be informed when they can register their device with our technicians on receipt of a completed reply slip.

E Safety

Some websites used in school may require registration. Students' school email accounts will be used for this. Forums may feature as part of approved websites. All students and parents are reminded of the importance of adhering to the principles of e-safety outlined below:

- keep personal information private
- consider the long-term implications of any content posted online
- do not upload or post inappropriate, offensive or illegal content to their own or other online spaces
- read and adhere to any website's terms of conditions of use – including those around age restrictions

E Learning is taught as part of the curriculum. There is a comprehensive guidance on e-safety on the http://www.getsafeonline.org/ website supported by the Department of Education. The Safeguarding Children section has a useful list of tips to ensure children are safe online.

13.4 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. They are from the National Cyber Security Centre (NCSC) glossary.

Term	Definition
Antivirus	Software designed to detect, stop, and remove malicious software and viruses.
Breach	When your data, systems or networks are accessed or changed in a non-authorised way.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks, or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services, and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems, and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Pharming	An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website address.

Term	Definition
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programmes designed to self-replicate and infect legitimate software programs or systems.
Virtual private network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly- targeted phishing attacks (where emails are made to look legitimate) aimed at senior people in an organisation.