Downe House

Policy

Information Systems

INFORMATION SYSTEMS ACCEPTABLE USE POLICY

Policy: All those in the school community using the school's Information Systems (IS) network shall adhere to strict guidelines concerning appropriate use of network resources and associated infrastructure.

Purpose: To define policies and procedures for accessing and utilising the school IS network and/or accessing the internet through the school IS network.

Scope: This policy applies to all users with access to the internet and related services through the school network infrastructure. Specifically, this includes, but not limited to, staff, pupils, governors and guest accounts.

Responsibilities: The Director of Digital Delivery and Innovation (DDDI) is responsible for reviewing and implementing this Information Systems Acceptable Usage Policy. All users are responsible for knowing and adhering to this usage policy.

1. POLICY STATEMENT

1.1 Unless otherwise stated in this policy, the use of all school-provided Information Systems and related services is specifically limited to activities in direct support of official school business. Digital platforms and internet access shall not be used for any illegal or unlawful purpose or otherwise in breach of this policy.

1.2 Information Systems shall be always used appropriately, and all communications must be professional and suitably reflective of the school's ethos. Access to school data must by via approved and authorised means only, and all data must be securely protected and subject to compliance with UK data protection law. Additional consideration must be given to the responsible and appropriate care, protection and safeguarding of the pupils, and the use of Information Systems managed accordingly.

1.3 If any user has a question of what constitutes acceptable use, staff should contact their line manager or contact the DDDI directly. Pupils should contact their Housemistress/ Housemaster or Tutor.

2. INAPPROPRIATE USE

2.1 Use of school email or other digital platforms shall not be used:

- to harass, intimidate, or otherwise annoy or bully another person.
- for commercial or political purposes. Fund-raising is permitted by prior agreement only. Charging arrangements for parents signing up to school activities is permitted.
- to attempt to circumvent or subvert security measures on either the school's network resources, or any other system connected to or accessible through the Internet.
- for access for interception of network traffic for any purpose other than engaging in authorised network administration.

- to make or use illegal copies of copyrighted material, store such material on school equipment, transmit or print such material over the school network. (e.g. images obtained on the internet).

3. DIGITAL COMMUNICATIONS (INCLUDING EMAIL, MICROSOFT TEAMS)

3.1. Digital communications include, but are not limited to, email and Teams messaging.
3.2. All users shall ensure all communication through school digital communications services is conducted in a professional manner. The use of suggestive, vulgar, or obscene language is prohibited.
3.3. Users shall not reveal, transmit or print private or personal information through digital communications services without clear and specific written approval from a member of the Leadership Team (LT).
3.4. Email and other digital communications are subject to filtering and monitoring in line with the school e-safety and Safeguarding and Child Protection policies.
3.5. Users should ensure that email messages are sent to only those users with a specific need to know. The transmission of email to large groups, use of email distribution lists, or sending messages with large file attachments should be avoided.
3.6. Email privacy cannot be guaranteed. For security reasons, messages transmitted through the school's email system or network infrastructure are the property of the school and are, therefore, subject to monitoring. Use of the school's email system automatically implies consent to monitor.
3.7. The school has arranged for an appropriate disclaimer to be appended to all email messages automatically that are sent to external addresses from the School, in order to provide necessary legal protection.
3.8. By default, all emails are retained for [at least] 3 years before deletion. Staff are required to retain emails related to essential or mission-critical projects. Emails that do not pertain to mission-critical projects or current issues should be deleted when they are no longer needed. Any details that are required to be kept beyond 3 years should be separately recorded outside of the email system.
3.9. Staff and pupils are expected to manage their mailbox size and keep within the allocated quota limit.
3.10. Users must not allow unauthorised access to the school's email services and facilities by third parties.
3.11. Users must not engage in any activities that could or are likely to corrupt or destroy other users' data.
3.12. Users must not create or transmit material which brings or is likely to bring the school into disrepute.
3.13. Emails containing attachments, hyperlinks or from an unfamiliar sender, are a likely source of cyber-attacks, viruses, or Malware. Users should contact the IS Support desk if they receive any such emails or they suspect their account may have been compromised. You should not click on any external links, or open attachments from unknown senders.
3.14. To protect against such cyber-attacks, the IS Support department will conduct periodic phishing simulation tests. Additional security training will be provided based on the results of such testing.

4. LAPTOPS / TABLETS (PERSONAL OR SCHOOL OWNED)

4.1. All pupils are required to adhere to this IS Acceptable Use Policy, as well as the E-Safety, Prevention of Bullying and Internet Social Networking Policy when using personal or school owned laptops or tablets ("computing devices.")
4.2. Pupils are responsible for their conduct when using computing devices. Any misuse of these computing devices by pupils will be dealt with under the school's Behaviour Management Policy, and with reference to the school's Safeguarding and Child Protection Policy as appropriate.
4.3. All computing devices (including personal laptops / tablets) used for schoolwork must be suitably password protected. Personal devices used by staff should only be used to access

school services, and the storage of personal or confidential school information on these devices is prohibited.

4.4. All new computing devices supplied by the school are configured appropriately prior to deployment.

4.5. Computing devices which are required for educational delivery shall be managed by the school, including the software build, permissions, filtering and inclusion of monitoring software for the purposes of managing the safeguarding of the pupil. This software and associated controls will be removed from a pupil's computing device when they leave the school.

4.6. Staff, parents and pupils should be aware that school email and internet usage (including through school Wi-Fi) will be monitored for safeguarding, conduct and performance purposes, and both web history and school email accounts may be accessed by the school where necessary for a lawful purpose – including serious conduct or welfare concerns, extremism and the protection of others. [Any personal devices used by pupils, whether or not such devices are permitted, may be confiscated and examined under such circumstances.]

4.7. Computing devices must not be left on view in an unattended vehicle; they should be placed in the boot or under cover to reduce the risk of theft.

4.8. The IS Support department may provide users with a loaned computing device, for example as a temporary replacement to support working whilst a faulty device is repaired.

4.9. Users who have been provided with a school owned computing device are expected to look after the equipment and take all reasonable care to avoid loss, damage, or theft. This also applies to peripheral equipment including, but not limited to, monitors, docking stations, styluses, and protective cases.

4.10. All computing devices should be kept in a protective case and a screen protector is highly recommended. Loaned computing devices issued by the IS Support department should not be removed from their protective cases.

4.11. If a member of staff loses their computing device, or the device becomes damaged or is stolen, Downe House reserves the right to pass all or some of the cost of replacement on to the member of staff involved. Accidental damage will only be covered in the first instance.

4.12. Ifa user's computing device is lost, stolen or mislaid, it must be reported immediately to the IS Support Department.

5. OTHER PORTABLE STORAGE DEVICES

5.1. The use of an external USB hard drive or similar device should be avoided if possible and must be discussed and agreed with IS Support prior to use. Encryption will be applied if necessary, and the device may need to be returned to IS Support for secure wiping of any stored data after use.

5.2. The copying of confidential or sensitive information to any external storage (including cloud storage) is not permitted. Where there are exceptional circumstances, such copying may only be created by the IS Support Department following written approval from the DDDI.

5.3. Portable devices must be stored securely when left unattended. Devices taken off-site should not be left unattended in public places.

5.4. If a portable storage device is lost, stolen or mislaid it must be reported immediately to IS Support.

5.5. The use of non-approved portable storage devices by staff will be subject to disciplinary action up to and including dismissal.

6. MOBILE PHONE DEVICES (PERSONAL OR SCHOOL OWNED)

6.1. During the school day staff and pupils are expected to exercise discretion in the use of mobile phone devices. As a general courtesy mobile phone devices should be turned off during such times or at least placed in 'silent' mode.

6.2. The school has the right to examine and / or confiscate any mobile phone device that it reasonably believes has been used to contravene this IS Acceptable Use Policy or has been used to engage in any other kind of misconduct.

6.3. Mobile phone devices are not permitted to use in either the Main dining room or the Willis dining room.

6.4. Ring tones in use should be appropriate for the school environment.

6.5. All internet usage via the school's systems and WIFI network is filtered and monitored by the school (see section 4.6 above which also applies to mobile devices).

6.6. Downe House is not liable for the loss or damage of personal mobile phone devices brought into the school.

6.7. Downe House prohibits the use of mobile phone devices or similar devices when the operation of such devices would be a distraction to the user and/or could create an unsafe environment, for example when operating machinery, working at heights or driving.

6.8. The following apply to all Downe House staff:

6.8.1. Staff should restrict personal calls during work time and should use personal mobile phone devices only during scheduled breaks or lunch periods in non-working areas. Other personal calls should be made during non-work time whenever possible, and staff should ensure that their friends and family members are made aware of this policy.

6.8.2. Downe House may issue mobile phone devices to employees for work-related communications. To protect the employee from incurring tax liabilities for the personal use of such equipment, these school issued mobile phone devices are to be used for business purposes only.

6.8.3. International roaming is blocked by default on school mobile phone devices. Staff needing to travel abroad for school related business must provide details of the trip to IS Support with the approval of their respective LT member.

6.8.4. Data plans for school mobile phone devices are not unlimited and are only intended to support the employee for work-related purposes. Staff should use wireless networking where possible to conserve mobile data. Staff will be liable for any excess data charges incurred which were not wholly in support of their work for the school.

6.8.5. All school mobile phone devices must be protected with PIN access enabled for initial access.

6.8.6. If a private mobile device is used to connect to the school network and systems, this device must then also be PIN protected for initial access.

6.8.7. It is the user's responsibility to ensure that any mobile devices (school or privately owned) have a strong password or PIN protection that is always required to be entered when accessing the device. The use of biometric access such as fingerprint or facial identification is also permitted.

6.8.8. Staff who have been provided with a school mobile phone device are expected to look after the equipment and take all reasonable care to avoid loss, damage, or theft. All devices should be kept in a protective case and a screen protector is highly recommended.

6.8.9. If a member of staff loses their mobile phone device or the device becomes damaged or is stolen, Downe House reserves the right to pass all or some of the cost of replacement on to the member of staff involved.

6.8.10. In cases of theft the member of staff will be required to advise the local police station of the circumstances of the theft and obtain an appropriate Police Incident Reference Number.

6.8.11. If a mobile phone device is lost, stolen or mislaid and it is used to receive school emails or is used to store school information then it must be reported immediately to the IS Support department.

6.8.12. Upon leaving the employment of the school, or at any time on request, a member of staff may be asked to produce their school owned mobile phone device for return or inspection.

6.8.13. Any member of staff unable to present their school owned mobile phone device in good working condition within a reasonable time may be expected to fund all or some of the cost of replacement.

6.8.14. Staff who leave the school with outstanding unauthorised charges made on a school mobile phone device may have such charges deducted from their final salary payment.

6.9. The following apply to all Pupils:

6.9.1. All pupils are required to adhere to this IS Acceptable Use Policy, as well as the E-Safety, Prevention of Bullying and Internet Social Networking Policy when using mobile phone devices.

6.9.2. Pupils are responsible for their conduct when using mobile phone devices. Any misuse of these devices by pupils will be dealt with under the school's Behaviour Management Policy, and with reference to the school's Safeguarding and Child Protection Policy as appropriate.

6.9.3. Pupils should not have mobile phone devices on display during the school day.

6.9.4. Further clarification for pupils regarding "Guidelines on the use of mobile phones" is available from the Housemistress.

7. PHOTOS/ VIDEOS ON ELECTRONIC DEVICES (PERSONAL OR SCHOOL OWNED)

7.1. Electronic devices include but are not limited to computing and mobile phone devices such as Microsoft Surfaces, tablets, laptops and mobile phones.

7.2. Pupils must not use any electronic device to take photos or videos at school without the explicit verbal consent of the individual being photographed or recorded, as well as a teacher.

7.3. The use of the electronic imaging function of electronic devices by a member of staff is prohibited in connection with any school business unless strictly carried out during a particular role at Downe House.

7.4. Staff may take photographs or videos of pupils on a school owned electronic device, provided it is done so in accordance with the school's policy on the use of images and strictly taken during their particular role at Downe House.

7.5. Under no circumstances should images or videos of pupils be taken by staff using privately owned equipment.

7.6. Staff may not take photographs and/or videos of pupils, on electronic devices in any 'private' areas e.g., bedrooms or bathrooms in boarding houses.

7.7. Transmission of any school information, logos, data, and/or photos of the premises or of any staff or pupils, contractors, subcontractors, or visitors is forbidden unless specifically authorised by the member of staff's line manager, unless such use forms part of the member of staff's role at the school e.g., Marketing / PR. It is a requirement that permission is sought from the appropriate authority or individual concerned before any imagery is captured.

8. CLOUD STORAGE

8.1. Staff are only permitted to use school provided cloud-based services for the storage of school related data (e.g. Microsoft OneDrive).

9. ONLINE LEARNING DELIVERY MICROSOFT TEAMS

9.1. Pupils should only use the chat functionality of Teams during lessons when explicitly invited to do so by staff.

9.2. As with all digital communication, Teams chat messages in both public and private groups are subject to monitoring by IS Support.

9.3. Unless authorized by the DDDI, channel post and chat messages cannot be modified or deleted. Such requests must be made through the IS Support desk.

9.4. Staff may use breakout rooms during lessons to facilitate discussion. Pupils should be aware that staff may drop in and out of breakout rooms without notice and that breakout rooms are also subject to recording.

10. SCHOOL WEBSITE (PUBLIC DOMAIN)

10.1. Pupils may create projects, artwork or writing which would be suitable for publication on the school website. The work will appear in an educational context on web pages with a copyright notice prohibiting the copying of such work without express written permission.

10.2. No personal information, other than their first name, will appear with such work, and particular care will be taken where photographs of pupils are being used on the school's

website. Personal pupil information including home address and contact details will always be omitted from the school's web pages.

10.3. Photographs will not be used under any circumstances where parents have specifically requested this.

11. PARENT ACCESS (for Parents and Guardians only)

11.1. A Parent Portal is provided by the school which allows greater freedom for publishing and showcasing pupils' work as it is private and only accessible by approved user authentication. This portal also contains a range of valuable information regarding policies, everyday activities at the school plus a summary of the academic record of each pupil.

12. PUPIL ACCESS

12.1. A Pupil Portal is provided which is primarily for use by the pupils, with staff providing much of the content.

12.2. Procedures are in place to monitor content; however, staff have a responsibility to ensure that only content appropriate to the year the student is in is uploaded and made available. Staff should liaise with the Administration team before uploading content.

12.3. Staff placing content on the school's digital platforms must also ensure that it complies with regulatory requirements. (Advice is available from the DDDI and the Administration team).

13. PRINTING

13.1. Pupils and staff are encouraged to digitally disseminate information via email or the School network, rather than printing, to reduce the environmental impact of printing.

13.2. All printing activity is monitored to ensure appropriate usage and correct allocation of costs to departments.

13.3. The ability to print may be withdrawn if misuse of printers and/or the associated consumables is identified. Examples of misuse include:

- Wasting resources e.g., wasting paper by printing multiple copies of the same document, wasting toner by printing documents with dark backgrounds
- Printing 'junk' i.e., clipart pictures with captions
- Printing anything that is deemed to be offensive.
- Printing large amounts of documents for personal use (i.e., not school work)

14. PERSONALLY IDENTIFIABLE INFORMATION ('PERSONAL DATA')

14.1. Personal data un-related to school business should not be kept on the school's computer network, cloud storage or within applications (e.g., personal bank details, private letters) unless there is an established school need and suitable data protection is in place.

14.2. The school is subject to UK data protection law – including the UK General Data Protection Regulation and Data Protection Act 2018 - which applies to the processing of personal data on school systems.

14.3. These systems include, but are not limited to, all data held within the school Management Information System, Emails, data stored on the school network and Microsoft OneDrive/SharePoint. Users must not remove and/or copy data from the school's system, unless authorised in writing by the DDDI.

14.4. If any member of staff is in doubt about what, if any, data may be removed or copied they should contact the DDDI.

14.5. If any member of staff is in any doubt about data protection issues, they should contact the DDDI.

14.6. If a pupil is in any doubt about data protection issues, they should contact their Housemistress / Housemaster or Tutor.

15. COMPUTER AND INTERNET USAGE – SECURITY

15.1. Staff who identify or perceive an actual or suspected security issue shall immediately contact IS Support and the DDDI.

15.2. Pupils who identify or perceive an actual or suspected security issue shall immediately contact their Housemistress / Housemaster or Tutor, who will in turn will contact the DDDI.

15.3. Users shall not reveal their account passwords to others (except to IS Support staff to facilitate resolving IS Support requests) or allow any other person, staff or pupil, to use their accounts. If a password is compromised it must be changed as soon as possible.

15.4. All use of IT assets is subject to monitoring by IS security procedures.

15.5. Access to school network resources shall be revoked for any user, staff or pupil, identified as a security risk or who has a demonstrated history of security problems.

15.6. The school operates an electronic filtering system to protect all users from inappropriate materials. This system logs all internet usage and email correspondence. The school maintains a right to consult these logs to help identify non-compliance with this policy or any other investigation that may be required. Some examples are given below:

- Establishing the existence of facts relevant to the school's business.
- Ensuring that the school's filtering system is working effectively in line with the school's Safeguarding and Child Protection Policy.
- Ascertaining or demonstrating standards which ought to be achieved by those using the facilities.
- Preventing or detecting crime.
- Investigating or detecting unauthorised use of email facilities.
- Ensuring effective operation of email facilities.
- To comply with any legal obligation.

15.7. Only software and services approved by the IS Department may be installed on or used by school connected devices. This ensures that the licensing of the software is appropriate and does not contravene licensing controls or data protection law. It also ensures that software is fully compatible with the school's computer systems.

15.8. Pupils are not permitted to arrange or conduct meetings online without the express permission of a teacher and/or parent.

15.9. If a pupil receives a message that causes them to feel uncomfortable in any way it must be reported to a teacher, their Housemistress/Housemaster or the DDDI. On no account should there be a response made to such a message.

15.10. If a staff member receives a message that causes them to feel uncomfortable, it must be reported to the DDDI. On no account should there be a response made to such a message.

15.11. Pupils must not access other pupils' files, folders or work for any reason.

15.12. The school reserves the right to examine or delete any files, communications (including email messages) and their attachments that may be held on its computer systems.

15.13. Staff and pupils should not expect that files stored on servers or storage media are always private. Computer logs may be viewed by the Headmistress or her nominated representative or the DDDI where misuse is suspected or detected.

15.14. Where access to the account and associated data of a member of staff is required without first gaining their approval, agreement to do so must first be sought from Human Resources.

16. SOCIAL MEDIA

16.1. All staff have access to social media providing the sites in question are approved and listed as permissible within the school's firewall.

16.2. All staff using social media must be aware of and comply with the School's Internet Social Networking Policy.

16.3. Pupils have access to a limited range of social media sites. This access is governed by time of day and according to the year the pupil is currently in.

16.4. Pupils and staff should be mindful and remain vigilant as to content posted on social media. Do not post any material including photographs and video clips that:

- Can be interpreted as bullying, embarrassing or distressing to another person.
- Brings the school into disrepute or be inappropriate for a professional who has the responsibility for the welfare, moral and ethical education of young people.
- Uses suggestive, vulgar or obscene language.

16.5. If any member of staff detects inappropriate content that affects the school community in any way or undermines its standing, they should report it immediately to the DDDI.

16.6. If any pupil detects inappropriate content that affects the school community in any way, they should report it immediately to their Housemistress / Housemaster or Tutor who will forward details of the incident to the DDDI.

16.7. The school reserves the right to contact any social media site used by anyone in the school community to investigate inappropriate use and where necessary request to have any such material removed.

17. COMPUTER AND INTERNET USAGE - PENALTIES

17.1. For the avoidance of doubt, creating, viewing, accessing, transmitting or downloading any of the following material will usually amount to gross misconduct (this list is a guide and not exhaustive):

- Pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature)
- Offensive, obscene, or criminal material or material which is liable to cause embarrassment to the school or those associated with it.
- A false and defamatory statement about any person or organisation
- Material, which is discriminatory, offensive, derogatory or may cause embarrassment to others (including material which breaches the school's policies on equal opportunities and anti-harassment and bullying)
- Confidential information about the school or any of its staff, governors, pupils, parents of pupils or alumni (except as authorised by the school or in the proper performance of staff or pupil duties)
- Any other statement which is likely to create any criminal or civil liability (for staff, pupils of the school)
- Material in breach of copyright, including plagiarism and the mis-use of tools such as Artificial Intelligence.

17.2. Any such action will be treated very seriously and is likely to result in summary dismissal / pupil expulsion as applicable.

17.3. Any violation of these policies or applicable UK laws while using the school's network shall be subject to loss of network privileges and any other disciplinary actions deemed appropriate, possibly up to and including dismissal in the case of staff or expulsion from the school in the case of pupils. Misuse of the school's network can in some circumstances be a criminal or civil offence and the school reserves the right to hand relevant information to the police or other relevant authorities in connection with any investigation in this regard. Appropriate criminal and/or civil prosecution may also be considered.

18. COMPUTER AND INTERNET USAGE - CONCLUSION

18.1. All terms and conditions as stated in this policy are applicable to all users of the school network and the Internet. These reflect an agreement of all parties and will be governed and interpreted in accordance with UK law.

19. This policy refers to the following School policies and procedures:

19.1. E-Safety
19.2. Safeguarding and Child Protection
19.3. Internet Social Networking Policy
19.4. Privacy Policy
19.5. IS Incident Handling (Procedure)
19.6. Behaviour Management Policy
19.7. Prevention of Bullying Policy

Acceptance Form

Please confirm that you understand and accept this policy by signing below and returning the signed copy to [insert relevant member of staff].

I understand and accept the School IS Acceptable Use Policy.

Please circle one of the below roles as appropriate

Staff Pupil Governor Other

Full Name _____

User Signature _____

Job Title (If staff) _____

Date _____

Revision History:

Revision	Date	Description of changes	Requested By
	March 2015	Initial Release of new format	S D Finch
	March 2016	9.0 amended to reflect current policy	S D Finch
	March 2017	No Changes	D McClymont
	January 2018	Updated to amalgamate several policies relating to acceptable use of various systems and infrastructure	D McClymont
	February 2019	Section 12, reflecting changing responsibility. GDPR acknowledgement	D McClymont
	February 2020	Reviewed	D McClymont
	February 2021	Updated to reflect new Pupil Hub and Parent Hub platforms. Addition of advice regarding Microsoft Teams. Addition of storage requirements from retired IS Data Storage policy. Additional guidance for handling of phishing emails. Addition of requirement to keep school owned devices in protective cases and clarification of chargeable damages.	A Jack
	February 2022	Reviewed	D McClymont
	February 2023	Reviewed	D McClymont
	December 2023	AI Guidelines Added	J Basnett
	February 2024	Reviewed	D McClymont
	September 2024	Various updates to realign and simplify after continuous progressive changes	C Kurn

Review Leader: Director of Digital Delivery and Innovation

Reviewed: September 2024

Next Review: September 2025