Downe House

INFORMATION SYSTEMS ACCEPTABLE USE POLICY

Policy: All those in the school community using the School's 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 IT network and/or accessing the Internet through the School IT 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 Information Systems (DIS) is responsible for reviewing and implementing this Information systems Acceptable Usage Policy.

The IS Network Manager (ISNM) is responsible for coordinating actions to meet the requirements of this policy.

All users are responsible for knowing and adhering to this usage policy.

The IS Network Manager is responsible for enforcing this policy.

1. ACCEPTABLE USE - COMPUTERS AND INTERNET

1.1. Access to the Internet is specifically limited to activities in direct support of official School business.

1.2. In addition to access in support of specific work related duties, the School's Internet connection may be used for private and recreational use in accordance with these guidelines.

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

2. INAPPROPRIATE USE - COMPUTERS AND INTERNET

2.1. Email and internet access shall not be for any illegal or unlawful purpose. Examples of this are the transmission of violent, threatening, defrauding, pornographic, obscene or otherwise illegal or unlawful materials.

2.2. Use of school e-mail or other messaging services shall be used primarily for the conduct of School business only. These services shall not be used to harass, intimidate or otherwise annoy another person.

2.3. The Internet may be accessed for private, recreational or any non-school-related activity within the guidelines of this policy.

2.4. The School's Internet and Intranet shall not be used for commercial or political purposes. Fund-raising is permitted.

2.5. The School's Extranet may not be used for commercial or political purposes. Charging arrangements for parents signing up to school activities is permitted.

2.6. Users shall not 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.

2.7. Users shall not use Internet access for interception of network traffic for any purpose other than engaging in authorised network administration.

2.8. Users shall not 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. Google images)

3. INTERNET AND E-MAIL USE

3.1. All users shall ensure all communication through school e-mail or internet messaging services is conducted in a professional manner. The use of suggestive, vulgar or obscene language is prohibited.

3.2. Users shall not reveal, transmit or print private or personal information through e-mail or internet messaging services without clear and specific written approval from a member of the Leadership Team (LT).

3.3. Email and Internet communications are subject to filtering and monitoring in line with the school e-safety and Safeguarding and Child Protection policies.

4. EMAIL SYSTEMS

4.1. Users should ensure that e-mail messages are sent to only those users with a specific need to know. The transmission of e-mail to large groups, use of e-mail distribution lists, or sending messages with large file attachments should be avoided.

4.2. E-mail privacy cannot be guaranteed. For security reasons, messages transmitted through the School's e-mail system or network infrastructure are the property of the School and are, therefore, subject to monitoring. Use of the school's e-mail system automatically implies consent to monitor.

4.3. The School has arranged for an appropriate disclaimer to be appended to all e-mail messages automatically that are sent to external addresses from the School, in order to provide necessary legal protection.

4.4. Staff are required to retain e-mails related to essential or mission-critical projects. E-mails that do not pertain to mission-critical projects or current issues should be deleted when they are no longer needed.

4.5. Staff and pupils are expected to manage their mailbox size and keep within the allocated quota limit.

4.6. School staff and pupils will ensure all communication through school e-mail is conducted in a professional manner. The use of vulgar, obscene, lewd, or suggestive language is prohibited. Use of such language is likely to be trapped by email electronic filters and offenders will be contacted accordingly.

4.7. Users must not allow unauthorised access to the School's e-mail services and facilities by third parties.

4.8. Users must not engage in any activities that could or are likely to corrupt or destroy other users' data.

4.9. Users must not create or transmit material which brings or is likely to bring the School into disrepute.

4.10. Emails containing attachments, hyperlinks or from an unfamiliar sender, are a likely source of cyber-attacks, viruses or Malware. Users should contact the Information

Systems department if they receive any emails that they suspect may have been compromised.

5. MOBILE PHONE DEVICES (PERSONAL OR SCHOOL OWNED)

5.1. During the school day staff and pupils are expected to exercise discretion in the use of mobile phone devices. As a general courtesy please turn the devices off during such times or at least place the phone in 'silent' mode

5.2. Staff should restrict personal calls during work time, and should use personal mobile phones 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.

5.3. Pupils should not have mobile phone devices on display during the course of the school day.

5.4. Staff and pupils are not permitted to use Mobile phone devices in either the Main dining room or the Willis dining room.

5.5. Staff and pupils should ensure that ring tones in use are appropriate for the school environment.

5.6. Downe House is not liable for the loss or damage of personal mobile phones brought into the school.

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

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

5.9. All school mobile phone devices and school supplied tablets must be protected with PIN access enabled for initial access.

5.10. If you use a private mobile device to connect to the school network and systems this device must then also be PIN protected for initial access.

5.11. It is the user's responsibility to ensure that any mobile devices (school or privately owned) have strong password or PIN protection that is always required to be entered when accessing the device.

5.12. Staff who have been provided with a School mobile phone are expected to look after the equipment and take all reasonable care to avoid loss, damage, or theft.

5.13. If a member of staff loses their mobile phone or the phone 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.

5.14. 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.

5.15. Upon leaving the employment of the School, or at any time on request, the member of staff may be asked to produce the mobile phone for return or inspection.

5.16. Any member of staff unable to present the phone in good working condition within a reasonable time period may be expected to fund all or some of the cost of replacement.

5.17. Staff who leave the school with outstanding unauthorised charges made on a school mobile phone will be considered to have left their employment on unsatisfactory terms and may have such charges deducted from their final salary payment.

5.18. Further clarification regarding "Guidelines on the use of mobile phones" can be found in Appendix 1.

6. MOBILE DEVICE CAMERAS (PERSONAL OR SCHOOL OWNED)

6.1. The use of the electronic imaging function of mobile devices is prohibited in connection with any school business unless strictly carried out in the course of your particular role at Downe House.

6.2. Staff may have photographs of pupils on a school-owned mobile device, providing they are strictly taken in the course of their particular role at Downe House.

6.3. Under no circumstances should images of pupils be taken using privately owned equipment, without the express permission of the DIS, DHM, BD or HM.

6.4. Where permission is granted the images should be transferred to School storage systems (server) and deleted from privately owned equipment (including cloud based storage) within one week of being taken.

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

6.6. 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.

7. SCHOOL WEBSITE (PUBLIC DOMAIN)

7.1. 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.

7.2. 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.

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

8. SCHOOL EXTRANET (for Parents and Guardians only)

8.1. The Extranet that is provided by the School allows greater freedom for publishing and showcasing pupils' work as it is private and only accessible by using an allocated username and password. This website also contains a range of valuable information regarding policies, every day activities at the School plus a summary of the academic record of each pupil.

8.2. The website address is https://extranet.downehouse.net. Personalised passwords and login credentials are provided to parents when the pupil joins the School.

9. SCHOOL INTRANET (for Pupils via 'Elaine')

9.1. 'Elaine' is primarily for use by the pupils, with staff providing much of the content. This application is accessible from within the School and from outside the School. Elaine is accessible to pupils and staff once they are logged in and authenticated with their school username and password.

9.2. 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.

9.3. Staff placing content on the Intranet must also ensure that it complies with regulatory requirements. (Advice is available from the Director of Information Systems and the Finance and Administration Bursar.

10. PRINTING

10.1. Pupils and staff are encouraged to digitally disseminate information via e-mail or the School network, rather than printing, to reduce the environmental impact of printing

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

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

10.3.1. Wasting resources e.g. wasting paper by printing multiple copies of the same document, wasting toner by printing documents with dark backgrounds

10.3.2. Printing 'junk' i.e. clipart pictures with captions

10.3.3. Printing anything that is deemed to be offensive

10.3.4. Printing large amounts of documents for personal use i.e. not school work

11. PERSONAL IDENTIFIABLE INFORMATION

11.1. Storage of such information should not be kept on the 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.

12. DATA PROTECTION ACT

12.1. The Data Protection Act 2018 and the General Data Protection Regulation (GDPR) was introduced to make new provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information. In accordance with the Act, the School only publishes pupils' information that is relevant to the context of the material.

12.2. By default all data stored on the School's computer systems is deemed the property of the School. These system's include, but are not limited to, all data held within the school Management Information System (MIS – Merlin), Emails, data stored on the school network and Microsoft OneDrive. Users removing and/or copying data from the School's system, unless authorised in writing by the Director of Information Systems, may be committing an offence under the Data Protection Act.

12.3. If any member of staff is in doubt about what, if any, data may be removed or copied they should contact the Director of Information Systems.

12.4. Staff are not permitted to store any school related data or information on external USB hard drives or memory sticks. Should such a storage device be required this should be discussed with the Information Systems department

12.5. Currently staff are only permitted to use cloud-based storage provided by Microsoft (One Drive), Google (Google Drive) and Apple (iCloud). Microsoft OneDrive is provided to all staff and pupils by Downe House. No other cloud storage service maybe used without the written permission of the Director of Information Systems.

12.6. Staff are not permitted to use any applications ("apps") or software packages on their mobile devices and/or tablets that store information in the "cloud" unless it is Microsoft OneDrive, Google Drive or Apple iCloud.

12.7. If any member of staff is in any doubt about data protection issues they should contact Director of Information Systems.

12.8. If a pupil is in any doubt about data protection issues they should contact their Housemistress / Housemaster or Tutor. If they are unable to answer the query then the query should be referred to the Director of Information Systems.

13. COMPUTER AND INTERNET USAGE – SECURITY

13.1. Staff who identify or perceive an actual or suspected security issue shall immediately contact the Director of Information Systems, in accordance with procedures laid down in the IS Incident Handling procedure.

13.2. Pupils who identify or perceive an actual or suspected security issue shall immediately contact their Housemistress / Housemaster or Tutor, they in turn will contact the Director of Information Systems in accordance with procedures laid down in the IS Incident Handling procedure.

13.3. Users shall not reveal their account passwords to others (except to IS Engineering staff to facilitate resolving IS Support Desk 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.

13.4. Any and all use of IT assets is subject to monitoring by IS security procedures.

13.5. 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.

13.6. 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:

13.6.1. Establishing the existence of facts relevant to the School's business.

13.6.2. Ascertaining or demonstrating standards which ought to be achieved by those using the facilities.

13.6.3. Preventing or detecting crime.

13.6.4. Investigating or detecting unauthorised use of email facilities.

13.6.5. Ensuring effective operation of email facilities.

13.6.6. To comply with any legal obligation

13.7. Only software approved by the IS Department may be installed on school connected devices. This ensures that the licencing of the software is appropriate and does not

contravene licensing controls. It also ensures that software is fully compatible with the School computer system.

13.8. All software used on school owned devices must be purchased through the IS Department. Staff wishing to install their own software, e.g. an iPad / cell phone application, need to seek permission from IT Support before installing so security and compatibility issues can be considered.

13.9. Pupils are not permitted to arrange or conduct meetings on-line without the express permission of a teacher and/or parent.

13.10. 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 Director of Information Systems. On no account should there be a response made to such a message.

13.11. If a staff member receives a message that causes them to feel uncomfortable, it must be reported to the Director of Information Systems. On no account should there be a response made to such a message.

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

13.13. 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.

13.14. 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 Director of Information Systems where misuse is suspected or detected.

14. SOCIAL MEDIA

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

14.2. All pupils using social media must be aware of and comply with the School's Internet Social Networking Policy for Girls.

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

14.4. 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. Current arrangements are available from the IS Network Manager.

14.5. 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:

14.5.1. Can be interpreted as bullying, embarrassing or distressing to another person.

14.5.2. 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.

14.5.3. Uses suggestive, vulgar or obscene language.

14.6. 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 Director of Information Systems.

14.7. 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 Director of Information Systems.

14.8. 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.

15. COMPUTER AND INTERNET USAGE - PENALTIES

15.1. For the avoidance of doubt, and without prejudice to paragraph 12.1 above, 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):

15.1.1. Pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature)

15.1.2. Offensive, obscene, or criminal material or material which is liable to cause embarrassment to the School or those associated with it

15.1.3. A false and defamatory statement about any person or organisation

15.1.4. 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)

15.1.5. 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)

15.1.6. Any other statement which is likely to create any criminal or civil liability (for staff, pupils of the School)

15.1.7. Material in breach of copyright.

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

15.3. 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.

16. COMPUTER AND INTERNET USAGE - CONCLUSION

16.1. 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.

17. This policy makes reference to the following School policies and procedures, copies of which can be located on Merlin in the 'My Policies' section:

17.1. E-Safety

17.2. Safeguarding and Child Protection

17.3. Internet Social Networking Policy for Girls

17.4. Internet Social Networking Policy for Staff

17.5. Privacy Policy

17.6. IS Incident Handling (Procedure)

Appendix 1 - Guidelines on the use of mobile phones

This document summarises the use of mobile phones in School. Further details can be found in House Handbooks and on the Parents Extranet in the section entitled 'Useful documents'. All electronic devices must be named and are brought to School at your own risk.

Mobile phones and other electronic devices should not be used in communal areas where they may disturb others e.g. the dining room or when walking around the School site.

Lower School

Remove

- Phones are kept by House all day during the week.
- Girls may access phones on their two calling nights each week and on weekends after lessons.
- Girls may access phones when out on trips if appropriate (e.g. for safety reasons).

Lower IV

- Phones are kept by House all day during the week except for during lunchtime and in the evening after supper.
- Girls may use their phone after lessons on the weekend.
- Girls may only take their phone out on trips if deemed appropriate (e.g. for safety reasons).
- Phones are handed in by 8pm each night.

Upper School

Upper IV

- Girls may keep their phone in their rooms during the day, but must not take their phones to lessons unless specifically requested to do so by a member of staff.
- Girls may use their phones in House during their free time i.e. break, lunchtime, tea and after supper. Girls should not use their phones during quiet time.
- Phones are handed in at 8.30pm.

Lower V

- Girls may keep their phone in their rooms during the day, but must not take their phones to lessons unless specifically requested to do so by a member of staff.
- Girls may use their phones in House during their free time i.e. break, lunchtime, tea and after supper. Girls should not use their phones during quiet time.
- Phones are handed in at 9pm until the Long Exeat of the Michaelmas term, after which, girls are permitted to keep their own device. Girls are encouraged to use their devices reliably and sensibly. If a girl is found to be misusing her device(s) or it is felt that use is negatively, affecting her well-being then the device(s) will be removed for a period. This is at the discretion of the Housemistress/master and Head of Section. Parents are always involved in this discussion.

Upper V

- Upper Fifth are permitted to keep their mobile phones and electronic devices with them on the understanding that they do not use them after lights out or in lessons unless specifically requested by a member of staff.
- If found using the devices irresponsibly, these may be confiscated.

Sixth Form

Mobile phone technology and electronic devices have their place in the classroom. If a girl needs to carry her phone during the working day, this should be on silent in lessons and taken out to use only when invited to do so by their teacher.

Acceptance Form

I understand and will abide by the School IS Acceptable Use Policy. I further understand that any violation of this policy may be considered unethical and may amount to misconduct or gross misconduct depending on the severity of the violation. It may also be a criminal or civil offence. Sanctions for breach may include removal of access privileges and /or disciplinary action (up to and including staff dismissal or pupil expulsion) as detailed above. Criminal or civil action may also be taken. Criminal proceedings can result in heavy fines and other penalties including imprisonment.

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	Section 12, reflecting changing responsibility. GDPR acknowledgement	D McClymont

This document makes reference to the following School policies, copies of which can be located on Merlin in the 'My Policies' section:

Equal Opportunities and Valuing Diversity (Reviewer: DHR)
Prevention of Bullying (Reviewer: DHM)

Review Leader: Director of Information Systems
Reviewed: February 2019
Next Review: February 2020