Downe House

Policy

Information Systems

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 Digital Delivery and Innovation (DDDI) 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 Digital Delivery and Innovation (DDDI) directly. Pupils should contact their Housemistress/Housemaster or Tutor.

2. INAPPROPRIATE USE - COMPUTERS AND INTERNET

2.1. Digital platforms 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 email or other digital platforms 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. 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 email or other messaging services such as Microsoft Teams 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 email or other messaging 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 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.
3.9. Staff and pupils are expected to manage their mailbox size and keep within the allocated quota limit.
3.10. School staff and pupils will ensure all communication through school email 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.
3.11. Users must not allow unauthorised access to the School's email services and facilities by third parties.
3.12. Users must not engage in any activities that could or are likely to corrupt or destroy other users' data.
3.13. Users must not create or transmit material which brings or is likely to bring the School into disrepute.
3.14. 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.
3.15. In order 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 personal laptops / tablets used for School work must be suitably password protected, especially when used in local mode off the network.
4.2. All laptops / tablets used on the School network need to be submitted IS Support to have data encryption enabled. All new laptops supplied by the School are configured appropriately prior to deployment.
4.3. Laptops / tablets must not be left on view in an unattended vehicle; place them in the boot or under cover to reduce the risk of theft.

4.4. The IS Support department may provide you with a loan device, for example as a temporary replacement to support working whilst a faulty device is repaired.
4.5. Staff who have been provided with a School owned 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 Surface type covers.
4.6. All devices should be kept in a protective case and a screen protector is highly recommended. Loan devices issued by the IS Support department should not be removed from their protective cases.
4.7. If a member of staff loses their 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.
4.8. If your device is lost, stolen or mislaid, it must be reported immediately to the IS Network Manager.

5. OTHER PORTABLE STORAGE DEVICES

5.1. If you require an external USB hard drive or similar device for use at School, the device needs to be registered with IT Support and have encryption put in place; it will also be allocated a School asset reference and marked accordingly. Only Downe House supplied devices are allowed on the School premises.
5.2. The copying onto CD/DVDs confidential or sensitive information is not permitted. Where there are exceptional circumstances such CD/DVDs may only be created by the IS Support Department following written approval from the DDDI.

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 please turn the devices off during such times or at least place the phone in 'silent' mode.
6.2. 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.
6.3. Pupils should not have mobile phone devices on display during the course of the school day.
6.4. Staff and pupils are not permitted to use mobile phone devices in either the Main dining room or the Willis dining room.
6.5. Staff and pupils should ensure that ring tones in use are appropriate for the school environment.
6.6. Downe House is not liable for the loss or damage of personal mobile phones brought into the school.
6.7. 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.
6.8. 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.
6.9. Data plans for School mobile devices are not unlimited and are only intended to support the employee for work-related purposes. You should use wireless networking where possible to conserve mobile data. You will be liable for any excess data charges incurred which were not wholly in support of your work for the School.
6.10. All school mobile phone devices and school supplied tablets must be protected with PIN access enabled for initial access.
6.11. 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.
6.12. 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.

6.13. 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. All devices should be kept in a protective case and a screen protector is highly recommended.
6.14. 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.
6.15. 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.
6.16. If your mobile phone / smart device is lost, stolen or mislaid (School or personal device) and it is used to receive school email or is used to store school information then it must be reported immediately to the IS Network Manager.
6.17. 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.
6.18. 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.
6.19. 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.
6.20. Further clarification regarding "Guidelines on the use of mobile phones" can be found in Appendix 1.

7. MOBILE DEVICE IMAGING (PERSONAL OR SCHOOL OWNED)

7.1. Mobile devices include, but are not limited to, cameras on Microsoft Surfaces, tablets, laptops and mobile phones.
7.2. 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.
7.3. Staff may have photographs or videos of pupils on a school-owned mobile device, providing they are strictly taken in the course of their particular role at Downe House.
7.4. Under no circumstances should images of pupils be taken using privately owned equipment, without the express permission of the DDDI, DH, AH(P) or HM.
7.5. Where permission is granted the images should be transferred to School storage systems (cloud) and deleted from privately owned equipment (including cloud-based storage) within one week of being taken.
7.6. 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.
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. USE OF USB MEMORY STICKS / PORTABLE MEDIA

8.1. USB memory sticks are small yet capacious. Their size makes them convenient to carry but also makes them easy to have stolen or to lose. A memory stick can contain thousands of documents and large databases.
8.2. It is also possible that if the stick is taken away from school and used on a virus infected PC, many corrupted documents may then be put back onto the School's network. At the very least you could lose a vital document.
8.3. Only school provided memory sticks may be used on the School network. These are secure in nature and require a password.
8.4. USB memory sticks are mass manufactured at low cost and are therefore frequently subject to failure. A USB memory stick should never constitute your only copy of the data.
8.5. Secure USB memory sticks are available from IS Support on request.
8.6. Any Staff users found using non-school issued portable devices will be subject to disciplinary action up to and including dismissal.
8.7. On receipt of a School secure memory stick, it must be registered with IS Support and an appropriate password put in place before the memory stick is taken away.

8.8. Key points that should be taken into consideration when considering using a USB storage device are listed below:
8.8.1. Why does the data need to be on a USB storage device?
8.8.2. If data is needed off site, why can't Remote Desktop access be used?
8.8.3. Could cloud based storage be used to access the data off-site?
8.8.4. Where is the data to be transferred to?
8.8.5. What type of information is to be stored?
8.8.6. Could any of the information be considered as personal?
8.8.7. Is any of the information relating to parents and in particular home address and contact information?
8.8.8. Is any of the information student identifiable and of a confidential nature?
8.9. Avoid using memory sticks to store any of your personal data e.g., bank details, PINS etc.
8.10. Ensure that portable devices are stored securely when left unattended. Devices taken off-site should not be left unattended in public places.
8.11. Ensure that information held on portable storage devices is backed-up on the School's network data facility.
8.12. If a portable storage device is lost, stolen or mislaid it must be reported immediately to the IS Network Manager.
8.13. Staff are responsible for ensuring that visitors or contractors who bring their own USB devices into the School (to give a presentation for example) are cleared by the IS Support department before being attached to the School network.
8.14. Staff must not bring personal USB storage devices to School.
8.15. Memory sticks issued by the School prior to September 2012 will not be valid and their continued use will contravene this procedure. Old memory sticks supplied by the School must be returned to IS Support.

9. CLOUD STORAGE

9.1. 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.

9.2. If a member of staff does decide to use cloud storage that is not provided by Downe House (OneDrive), no School sensitive data, pupil data or other confidential information is permitted to be stored in the cloud.

9.3. Also, some of the smaller cloud storage companies may not always be financially sound; it they fail, control of our data may be lost.

9.4. NB: Data stored in the Cloud will not be updated or linked to dynamically changing data held on SchoolBase which is likely to make its use for decision making unreliable.

10. ONLINE LEARNING DELIVERY MICROSOFT TEAMS

10.1. To support digital learning, staff may deliver and record lessons via Microsoft Teams. Any such recordings should be stored in Microsoft Stream, OneDrive or SharePoint.

10.2. Pupils should only use the chat functionality of Teams during lessons when explicitly invited to do so by staff.
10.3. As with all digital communication, Teams chat messages in both public and private groups are subject to monitoring by IS Support.
10.4. 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.
10.5. 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.

11. SCHOOL WEBSITE (PUBLIC DOMAIN)

11.1. 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.

11.2. 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.

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

12. SCHOOL PARENT HUB (for Parents and Guardians only)

12.1. The Parent Hub 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, everyday activities at the School plus a summary of the academic record of each pupil.

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

13. SCHOOL PUPIL HUB

13.1. The 'Pupil Hub' 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. The 'Pupil Hub' is accessible to pupils and staff once they are logged in and authenticated with their school username and password.

13.2. 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.

13.3. Staff placing content on the School's digital platforms must also ensure that it complies with regulatory requirements. (Advice is available from the Director of Information Systems and the Administration team).

14. PRINTING

14.1. 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.

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

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

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

14.3.2. Printing 'junk' i.e., clipart pictures with captions

14.3.3. Printing anything that is deemed to be offensive.

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

15. PERSONAL IDENTIFIABLE INFORMATION

15.1. 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.

16. DATA PROTECTION ACT

16.1. 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.

16.2. By default, all data stored on the School's computer systems is deemed the property of the School. These systems include, but are not limited to, all data held within the school Management Information System (MIS – SchoolBase), Emails, data stored on the school network and Microsoft OneDrive/SharePoint. 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.

16.3. 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.

16.4. 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.

16.5. Currently staff are only permitted to use cloud-based storage provided by Microsoft (OneDrive), 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.

16.6. 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.

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

16.8. 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.

17. COMPUTER AND INTERNET USAGE – SECURITY

17.1. 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.

17.2. 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.

17.3. Users shall not reveal their account passwords to others (except to IS Support 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.

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

17.5. 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.

17.6. 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:

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

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

17.6.3. Preventing or detecting crime.

17.6.4. Investigating or detecting unauthorised use of email facilities.

17.6.5. Ensuring effective operation of email facilities.

17.6.6. To comply with any legal obligation.

17.7. 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.

17.8. 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 IS Support before installing so security and compatibility issues can be considered.

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

17.10. 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.

17.11. 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.

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

17.13. 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.

17.14. 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.

18. SOCIAL MEDIA

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

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

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

18.4. 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.

18.5. 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:

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

18.5.2. 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.

18.5.3. Uses suggestive, vulgar or obscene language.

18.6. 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.

18.7. 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.

18.8. 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.

19. COMPUTER AND INTERNET USAGE - PENALTIES

19.1. 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):

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

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

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

19.1.4. 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)

19.1.5. 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)

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

19.1.7. Material in breach of copyright.

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

19.3. 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.

20. COMPUTER AND INTERNET USAGE - CONCLUSION

20.1. All terms and conditions as stated in this policy are applicable to all users of the school network and the Internet – including the use of AI, see Appendix 2 for further information. These reflect an agreement of all parties and will be governed and interpreted in accordance with UK law.

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

21.1. E-Safety
21.2. Safeguarding and Child Protection
21.3. Internet Social Networking Policy for Girls
21.4. Internet Social Networking Policy for Staff
21.5. Privacy Policy
21.6. 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 Parent Hub 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.

Remove

- Phones are kept by Housestaff all day during the week.
- In the evening, after supper, girls may request to use their phone for up to 30 minutes (before 7.45pm). Phones are not allowed to be taken to dormitories.
- Girls may take their phones with them to any away Games matches.
- Girls may access phones when out on trips if appropriate (e.g. for safety reasons).
- At the weekends girls may have access to their phones for up to an hour each day.
- Phones and other devices with internet access such as tablets, smart watches and games consoles are handed in by 7.45pm each night.

Lower Fourth

- Phones are kept by Housestaff all day during the week.
- In the evening, after supper, girls may request to use their phone for up to 30 minutes (before 7.45pm). Phones are allowed to be taken dormitories.
- Girls may take their phones with them to any away Games matches.
- Girls may access phones when out on trips if appropriate (e.g. for safety reasons).
- At the weekends girls may have access to their phones for up to an hour each day.
- Phones are handed in by 8pm each night.

Upper Fourth

- Phones are kept by Housestaff at all times, except for the following periods:
    - Monday – Thursday: 6.30 – 7.30pm
    - Friday: 8.15 – 8.45am and 6.30 – 8.30pm
    - Saturday: 12 – 5pm
    - Sunday: 9-10am and 5 – 8.30pm
- Weekend activities: Girls will be able to take their mobile phones to some activities where needed or beneficial; this will be decided according to the event/activity.

Lower Fifth

- Girls are requested to hand their phones in to Housestaff during the day. They 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. lunchtime and after supper. Girls should not use their phones during Quiet Time.
- Phones are handed in at 9pm. 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 wellbeing, then the device(s) will be removed for a period. This is at the discretion of the Housemistress and Assistant Head (US). Parents are always involved in this discussion.

Upper Fifth

- UV are permitted to keep their mobile phones and electronic devices with them during the day, on the understanding that they do not use them in lessons unless specifically requested by a staff member.
- After the Long Exeat in the Lent term, girls may keep their device overnight on the understanding that they do not use them after lights out. This privilege is at the discretion of the Assistant Head (US).
- If found using the devices irresponsibly, these may be confiscated.

Sixth Form

Sixth Form students are permitted to keep their mobile phones and electronic devices with them. However, girls should still obey the general rules surrounding devices and not use these in communal areas where they may disturb others and not in the Dining Room.

Overseas Families

Alternative arrangements will always be accommodated for girls whose families are based overseas, to be agreed with the Housemistress.

Appendix 2 – AI GUIDELINES

AI Overview

In the rapidly evolving landscape of education, Artificial Intelligence (AI) has emerged as a transformative tool. AI, in this context, refers to computer systems and software that can perform tasks that typically require human intelligence, such as understanding natural language, recognising patterns, and making decisions. These AI tools, including language models like ChatGPT, offer immense potential in enhancing the learning experience. The following guidelines are designed to provide students and teachers at Downe House with a clear framework for the responsible and ethical use of AI in education. They aim to ensure that while we harness the benefits of AI, we also maintain academic integrity, protect privacy, and foster an environment of critical thinking and originality. These guidelines serve as a roadmap for integrating AI into our educational practices, ensuring that it complements rather than replaces the human elements of teaching and learning.

AI Guidelines for students

1. AI Usage: Be transparent
Show academic honesty by acknowledging and citing any AI technology used in your work. Failing to do so goes against academic principles. **(Section 8.3d Behaviour Policy)**
How to cite: ChatGPT 3.5 (https://openai.com/blog/chatgpt/), 25/01/2023.

2. Responsible Use of AI: Do not cheat
AI tools must not be used for cheating, plagiarism, or any other behaviour which is harmful to you or anyone else. **(Section 8.3d Behaviour Policy)**

3. Original Effort: AI is a guide, not an author
AI-generated content should complement your effort and understanding. Ensure that your work is unique and reflects your understanding of the material.

4. Accuracy: check AI output for accuracy
Verify the accuracy of information received from AI language models (e.g., ChatGPT). Do not rely solely on the chatbot's output; critically assess and validate the information.

5. Responsibility: Reference AI when using it.
You are responsible for your AI technology usage. If you use AI to help with schoolwork, make sure you tell your teacher. Do not pretend that work from AI is your own.

6. Confidentiality & Privacy: Don't share private information
Maintain the confidentiality of your interactions with AI tools like ChatGPT. Refrain from sharing any sensitive or personal information about yourself or others with the chatbot.
(Section 3.3.3 of the IS Acceptable Use Policy)

7. Monitoring and Consequences
Teachers at Downe House will monitor AI usage to ensure compliance with these guidelines. Breaching this policy may result in disciplinary action following the school's sanctions' framework.

8. **Ethical Use of AI in Media Creation**: Use AI tools, including those for creating images or videos, ethically and responsibly. Do not create or distribute misleading, deceptive, or harmful content. Always respect the rights and dignity of others in your digital creations. Misuse may result in disciplinary action following the school's sanctions' framework.

Sixth Form: Please see guidance below from JCQ relating to NEA Assessments and UCAS applications.

These guidelines will be reviewed to ensure they remain current, incorporating technological advancements and the latest educational best practices.

AI Guidelines for teachers

1. Use AI as a supplementary tool in teaching and ensure that AI-generated content or suggestions are used to complement, not replace, your expertise and instructional material.
2. Critically assess the accuracy of information provided by AI language models. Incorporate AI suggestions after ensuring their relevance and correctness in the educational context.
3. Be aware of the potential biases and inaccuracies in generative AI tools and educate students about these risks. Discuss with students how biases can affect information quality and the ethical considerations in using such tools.
4. Be transparent about the use of AI in preparing and delivering educational content. Cite the use of AI tools where appropriate (e.g. if creating a model essay) and discuss their usage openly with students.
5. Handle all data, especially student information, with confidentiality and care. Be cautious of sharing sensitive data with AI tools and ensure compliance with data protection regulations and school policies.
6. Understand that the school will monitor the use of AI tools to ensure adherence to these guidelines. Non-compliance may be addressed according to the school's code of conduct.
7. Educate and guide students in the responsible use of AI, echoing the principles laid out in their guidelines, to foster a culture of integrity and ethical technology use.
8. Collaborate with colleagues in sharing experiences and strategies for effective AI integration in teaching, fostering a community of shared learning and innovation.
9. Be acquainted with JCQ guidelines (see summary below), to provide informed guidance and maintain academic integrity.

JCQ Guidance on use of AI in Assessments

There are tight regulations in respect to subjects with non-exam assessments (NEA) and where a subject has a NEA element. The following from the JCQ guidelines should be read carefully.

JCQ-AI-Use-in-Assessments-Protecting-the-Integrity-of-Qualifications.pdf
While the potential for student artificial intelligence (AI) misuse is new, most of the ways to prevent its misuse and mitigate the associated risks are not; centres will already have established measures in place to ensure that students are aware of the importance of submitting their own independent work for assessment and for identifying potential malpractice. This guidance reminds teachers and assessors of best practice in this area, applying it in the context of AI use.

The guidance emphasises the following requirements:

• As has always been the case, and in accordance with section 5.3(j) of the JCQ General Regulations for Approved Centres (General Regulations - JCQ Joint Council for Qualifications), all work submitted for qualification assessments must be the students' own;
• Students who misuse AI such that the work they submit for assessment is not their own will have committed malpractice, in accordance with JCQ regulations, and may attract severe sanctions;
• Students and centre staff must be aware of the risks of using AI and must be clear on what constitutes malpractice;
• Students must make sure that work submitted for assessment is demonstrably their own. If any sections of their work are reproduced directly from AI generated responses, those elements must be identified by the student and they must understand that this will not allow them to demonstrate that they have independently met the marking criteria and therefore will not be rewarded (please see the Acknowledging AI Use of the policy);
• Teachers and assessors must only accept work for assessment which they consider to be the students' own (in accordance with section 5.3(j) of the JCQ General Regulations for Approved Centres); and
• Where teachers have doubts about the authenticity of student work submitted for assessment (for example, they suspect that parts of it have been generated by AI but this has not been acknowledged), they must investigate and take appropriate action.

The JCQ awarding organisations' staff, examiners and moderators have established procedures for identifying, reporting and investigating student malpractice, including the misuse of AI.

The JCQ awarding organisations are continuing to monitor developments in this area and will update this guidance when appropriate.

Acknowledging AI Use - for Non-examined assessments.

JCQ-AI-Use-in-Assessments-Protecting-the-Integrity-of-Qualifications.pdf
Where AI tools have been used as a source of information, a student's acknowledgement must show the name of the AI source used and should show the date the content was generated. For example: ChatGPT 3.5 (https://openai.com/blog/chatgpt/), 25/01/2023. The student must, retain a copy of the question(s) and computer-generated content for reference and authentication purposes, in a non-editable format (such as a screenshot) and provide a brief explanation of how it has been used.

This must be submitted with the work, so the teacher/assessor is able to review the work, the AI-generated content and how it has been used. Where this is not submitted, and the teacher/assessor suspects that the student has used AI tools, the teacher/assessor will need to consult the centre's malpractice policy for appropriate next steps and should take action to assure themselves that the work is the student's own. Further guidance on ways this could be done are set out in the JCQ Plagiarism in Assessments guidance document (see link below).

UCAS guidance

UCAS provides clear guidance on using AI such as ChatGPT.

Its web page on the topic covers the following points:

- What is AI & ChatGPT
- Tips for using AI and ChatGPT with your personal statement.
- Is using AI to help with my personal statement 'cheating' (shared below)

Is using AI to help with my personal statement 'cheating'?

As you can imagine, we have had a lot of questions from people applying for university or college about whether using tools like ChatGPT to help with your UCAS personal statement is considered 'cheating'.

Generating (and then copying, pasting and submitting) all or a large part of your personal statement from an AI tool such as ChatGPT, and presenting it as your own words, could be considered cheating by universities and colleges and could affect your chances of an offer.

When you complete your application, you now have to declare that your personal statement hasn't been copied or provided from another source, including artificial intelligence software.

As part of our responsibility to applicants and universities and colleges, the UCAS Verification Team run checks to detect fraudulent applications and patterns of similarity in personal statements. Read our guide to fraud and verification and similarity.

If UCAS anti-plagiarism software detects elements of a personal statement that are similar to others, the universities or colleges it is intended for may be notified.

The personal statement is exactly that; personal. It should describe your ambitions, skills and the experiences that make you suitable for the course you're applying for in your own words. A lot of students we speak to say the process of writing it helps confirm that they're applying for the right course.

If your personal statement doesn't appear genuine, it could affect your chances of being offered a place. AI is good but it can't replicate your personal thoughts and feelings and convey your own skills and experiences. A bland AI-generated personal statement is not what universities and colleges are looking for.

However, universities and colleges do understand that AI tools can be useful to applicants writing personal statements if used in the correct way. We have outlined some useful tips on using such tools below.

Access the full page here:

A guide to using AI and ChatGPT with your personal statement | Undergraduate | UCAS

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 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

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

Equality, Diversity and Inclusion and Belonging (Reviewer: DHR)

Prevention of Bullying (Reviewer: DH)

Review Leader: Director of Digital Delivery and Innovation

Reviewed: February 2024

Next Review: February 2025