

Dunottar School

Pupil IT Acceptable Use Policy

Dunottar School – Pupil IT Acceptable Use Policy

Document Control	
Document Title:	Pupil Acceptable Use Policy
Version:	1.0
Summary of Changes from Previous Version:	<ol style="list-style-type: none"> 1. Policy moved across to the new template 2. No longer known as Acceptable Use of Technology for Students. 3. Addition on acceptable use of IT 4. Playing of online games permitted in certain circumstances.
Name of Originator/Author (including job title):	Tom Stevens, Network Manager
Target Audience:	Pupils
Name of Individual/department responsible:	T.Stevens
Review By Date:	January 2027
Date Issued:	January 2025



Table of Contents

1.	Policy Introduction	1
2.	School Computers	1
3.	Internet Access.....	1
4.	Security and Privacy	2
5.	E-mail	2
6.	Photographs and Video.....	2
7.	Appropriate Use of AI	3
8.	IT Acceptable Use Policy Agreement	3



1. Policy Introduction

- 1.1 This policy is built around the idea that you, as pupils of Dunottar School, will respect and protect yourselves, the school, and the school community in your use of technology. Every time you use technology or connect to the internet, you need to be aware of the possibilities available to you, how to behave responsibly and how to stay safe. This policy applies to all members of our school community including but not limited to staff, students, governors, volunteers and visitors.
- 1.2 It is important that your actions show respect to anyone who could see your presence online, whether they are directly known to you or not. Equally, you must ensure that you limit your audience only to those who you want to view your content wherever possible. Your online presence (digital footprint) should always be a positive one, as should your use of technology in school.

2. School Computers

- 2.1 Do not install, attempt to install, or store programs/software of any type on the computers or Microsoft 365 cloud storage without permission.
- 2.2 Do not damage, disable, or otherwise harm the operation of computers or their associated peripherals.
- 2.3 Do not intentionally waste resources. This includes use of the school's printers, which should only be for educational purposes.
- 2.4 Do not eat or drink near computer equipment.
- 2.5 Respect and do not attempt to bypass security in place on the computers or attempt to alter any of the settings.
- 2.6 The use of personal computing devices is bound by the Bring Your Own Device (BYOD) policy.
- 2.7 Do not write or publish anything using any device or computer that you would not be prepared to show your parents, the headmaster, or a future employer.
- 2.8 Do not be obscene either in the words that you use or the content that you view. This includes material that is violent, racist, or adult in nature.
- 2.9 Respect the laws of copyright and ensure that sources used are referenced appropriately.
- 2.10 Do not share content that puts you or anyone else at risk in any way. This includes revealing passwords, personal details, photos, or your location. Tell an adult if someone asks you for any of these details.

3. Internet Access

- 3.1 Do not access the internet unless for study or for school-authorised/supervised activities.
- 3.2 Do not use the internet to obtain, download, send, print, display, or otherwise transmit or gain access to materials which are unlawful, obscene, abusive, or hurtful to others or which may bring the school into disrepute.

- 3.3 Do not attempt to circumvent the school's filtering in any way.
- 3.4 Do not engage in 'chat' or social networking activities over the internet.
- 3.5 Never arrange to meet anyone unless accompanied by a parent or guardian. People that you meet online are not always who they appear to be.
- 3.6 The playing of online games is not permitted at any time whilst on the school site unless explicit permission is given by the school's IT department or by your teacher.

4. Security and Privacy

- 4.1 Do not disclose your password to anyone else or use passwords intended for the use of others.
- 4.2 Never tell anyone that you connect with on the internet your home address, telephone number, or school name, or send photographs of yourself or others, unless you are given permission by a member of staff to do so.
- 4.3 Staff may review files and communications on school equipment and owned systems to ensure that users are using the system responsibly.

5. E-mail

- 5.1 Be polite and appreciate that other users might have different views. The use of strong language, swearing or aggressive behaviour is not allowed.
- 5.2 The sending or receiving of emails containing material likely to be unsuitable for children or schools is strictly forbidden. This applies to any material of a violent, dangerous, racist, or inappropriate content.
- 5.3 Only use the school-based email system and Microsoft 365 to store your work. Do not send schoolwork home via personal email accounts.
- 5.4 When contacting staff via email, this should only be done using your school email account. Emails sent from a pupil's personal email address will not be responded to.
- 5.5 Do not download or open file attachments unless you are certain of both their content and origin and trust the sender. File attachments may contain viruses that could cause loss of data or damage to the school network or equipment. If you are sent any inappropriate or upsetting material report it immediately to the Network Manager or the Deputy Head (Pastoral).

6. Photographs and Video

- 6.1 Do not take pictures or record film of any pupils or members of staff, while in school or on school trips, without the permission of those being photographed or filmed.
- 6.2 If you need to photograph or film other pupils as part of an educational activity (e.g. drama rehearsal), you should use school equipment and you must seek permission from a teacher to make the film and check that pupils involved give their consent.

- 6.3 Where personal devices are used, such as on school trips with general permission from the trip leader, consideration should be given to the appropriateness of uploading pictures or film to social media and, if requested by the subject of the images, you must remove them from social media platforms. Uploading inappropriate photos or videos will result in disciplinary action.
- 6.4 Never send, print, display, or otherwise transmit images which are unlawful, obscene, abusive, or hurtful to others, including youth-produced sexual imagery content, or which may bring the school into disrepute.
- 6.5 Do not use the school devices for taking images of other pupils unless it forms part of a specific lesson.
- 6.6 Report immediately to your teacher any images on a school iPad which you deem to be inappropriate.

7. Appropriate Use of AI

- 7.1 Use AI tools responsibly and ethically. Do not use AI to generate inappropriate, harmful, or misleading content.
- 7.2 Ensure that any AI-generated content is clearly identified as such and does not violate copyright laws.
- 7.3 Using AI to generate content and submitting it as your own work is considered plagiarism.
- 7.4 Do not use AI to impersonate others or to create fake identities.
- 7.5 Use AI to enhance your learning and creativity, but always verify the information provided by AI tools with reliable sources.
- 7.6 Report any misuse of AI tools to a member of staff.

8. IT Acceptable Use Policy Agreement

- 8.1 You must read and submit the electronic form before you can be allowed to use the school's ICT resources.
- 8.2 You must agree to the school viewing your school account, with just reason and without notice, any emails you send or receive, material you store on the school's computers, or logs of websites you have visited.
- 8.3 You must only access those services you have been given permission to use.
- 8.4 You may bring your personal devices such as laptop into school to work on where you have permission from staff. You will only be able to access the schools Wi-Fi by installing some certificates onto your device. The IT department can help with this.
- 8.5 You must adhere to all instructions set out in this Acceptable Use Policy.
- 8.6 You must also abide by the school's Bring Your Own Device (BYOD) policy where applicable.
- 8.7 If you become aware of a breach of this policy, it is your responsibility to report it to a member of staff.

- 8.8 You are reminded that the use of ICT in school is a revocable privilege and not a right. Where the rules are broken and/or misuse has occurred you may lose the right to use ICT in school and/or face sanctions. For serious breaches the involvement of the police may be necessary.
- 8.9 **Penalties for misuse of computer systems under the Computer Misuse Act 1990 and the Data Protection Act 2018 will depend on the nature and seriousness of the offence. Disciplinary action may be taken against pupils who contravene this policy. The school, for various legitimate reasons, may need to monitor the use of email and internet access from time to time.**

Name of owner	T.Stevens	
Governor responsible	Dan Hawker	
Date Document Approved	January 2025	T.Stevens
Date document reviewed		T.Stevens
Next Review date	January 2027 or when events or legislation require	