



SHERBORNE BOYS

Acceptable Use of ICT Policy

Approving body: SLT

Owner: ICT

Author: Director of ICT Services

Executive Summary

This document outlines the school's ICT Acceptable Use Policy designed to ensure responsible and safe use of digital technology by pupils. It covers the expectations, restrictions, and responsibilities related to using school and personal ICT devices within the educational environment.

Date of Review: Michaelmas 2025
Date of Approval: 29 October 2025



Issue Number: 7
Review Due: Michaelmas 2026

Contents

Introduction.....	2
All pupils are required to understand and agree that:	2
Laptops and Mobile Devices in School.....	4
Appendix 1: Summary of Changes	4

Introduction

ICT is an important part of learning, and it is essential that all pupils behave responsibly and know how to stay safe when using it. The intention of this Policy is to ensure that pupils use digital technology sensibly and legally and to protect them from inappropriate attention or unsuitable material.

Pupils and parents are asked to read this ICT Acceptable Use Policy carefully, to discuss it and then to sign the agreement in the New Pupils' Pack. Any concerns can be discussed with the Director of ICT Services.

Once you and your son have signed the Policy, your signatures will indicate acceptance of the Policy (and any subsequent iterations) for the whole time that your son is at the School. The aim and spirit of the Policy will stay the same from year to year, but the School reserves the right to change the wording of some of the technical details in order to take account of any recent developments in ICT, legislation, and best practice. Pupils will be kept informed of any changes.

All pupils are required to understand and agree that:

1. References to ICT in this policy include all electronic Information and Communications Technologies, including network connections, Wi-Fi, the internet, email, social media, mobile technologies, and online resources including the use of Generative and other forms of Artificial Intelligence (AI).
2. Unless specified otherwise, this policy applies equally to the use of equipment owned by pupils as it does to equipment provided by the School.
3. Access to the School's ICT facilities is provided primarily in support of educational research and learning. Academic use takes priority at all times.
4. The School has a legal duty to protect and safeguard the pupils, and reserves the right to monitor, record and store a record of ICT use. This information may be used to prevent cases of inappropriate, unethical, or illegal activity, or provide evidence to authorities if required.
5. Pupils must refrain from accessing any content that would be considered as offensive by the School or their parents/guardians, including (but not limited to) pornographic, extremist, racist, violent, sexist, defamatory, blasphemous, or other offensive or unacceptable material. Pupils are responsible for reporting to the School any such material if it is accessed inadvertently.

6. The use of mobile data networks on personal devices is prohibited, as this could place pupils at significant risk and also risks compromising the School's network security and protection.
7. The use of VPN (Virtual Private Network) software on devices is strictly prohibited within the School. Any installation of this type of software will automatically prevent the device from connecting to the School's wireless network and will be an impediment to learning and teaching.
8. All passwords, whether for School accounts, personal social media accounts, or mobile devices, must be kept secure and a pupil may only use School facilities whilst logged on with his correct username and password.
9. Pupils must not allow others to use their username and password and they must not leave a computer unattended whilst logged on.
10. The School email system is the preferred form of email to be used from within the School. School emails are filtered and may be monitored for forbidden content. Personal email accounts should not be used for school communication.
11. Pupils may only use "social media" outside of working hours.
12. Pupils must use social media responsibly and must not reveal sensitive or personally identifiable information about themselves or others. Particular care must be taken not to share information or photographs which would cause offense or embarrassment if they became public.
13. Pupils must not use image manipulation software to create and/or share indecent images of other people. Any such activity will be, where necessary, reported to the Police.
14. Pupils must not use any technology to impersonate another person.
15. Pupils must take particular care online to respect other people, including other pupils, and must not act in ways which might cause offence or upset.
16. Pupils must be courteous and use appropriate language in all electronic communication. Note also that the law of libel is applicable online.
17. Pupils must respect copyright laws and intellectual property rights.
18. Pupils must accept that plagiarism is always unacceptable, including copying material from other pupils and claiming it as their own work. They must not access websites that encourage plagiarism or other academic dishonesty. They may only use downloaded materials in an appropriate manner in their work, listing it in a bibliography and clearly specifying quoted material.
19. Pupils may make responsible use of AI, subject to the guidance of their teachers and any restrictions that the School may impose from time to time. AI must never be used to replace critical thinking or to submit work to teachers or examination bodies as being work of their own making. Pupils may use AI tools for pieces of work if the teacher has permitted it, but pupils must ensure that they do not use AI to the detriment of their understanding of the material. In addition, pupils will be asked to undertake training in the use of AI in accordance with the school's AI policy, whether that be for their general education or for submitting work for assessment purposes.
20. Pupils must not seek to obtain or view illegally pirated media, software, or other material.
21. Pupils must not tamper with files, passwords or other types of data or electronic media belonging to other users.
22. Pupils must not damage either the hardware or software of any computer systems.

23. Pupils must not attempt to gain entry to any systems or data that they do not have explicit authorisation to access or use any hardware or software on the network to assist in gaining entry.
24. Pupils must not use any School resources for personal commercial gain.
25. Pupils must not attempt to install, store, or use unauthorised software on any School equipment, including the School network.
26. In bringing their own equipment such as 'phones, laptops or tablets into School or the House, pupils agree to allow and assist access to the data upon them by Housemasters or other senior staff where required as part of a disciplinary investigation.
27. The School accepts no liability for any loss or damage to any equipment the pupils bring to school.
28. Pupils agree to install the classroom.cloud pupil software on the devices that they use in a scheduled class and agree not to uninstall this software so that it can be utilised by teachers to aid in improving teaching and learning.

Failure to abide by the above policy is likely to lead to restrictions to access of the School's facilities and may lead to other sanctions including, in the most serious cases, expulsion from the School.

Laptops and Mobile Devices in School

Pupils may bring their mobile devices into School on the understanding that they are only to be used in accordance with the School mobile device and acceptable use policies. They can connect to the School network using wireless connections throughout the boarding houses, buildings, and grounds. Such devices may be connected to the School network provided they meet a minimum specification.

Parents must accept that if they provide or allow their son to purchase or use 3G/4G/5G devices that it will be impossible for the School to monitor pupil internet usage and safety. The parents must accept responsibility for any unfiltered usage.

Appendix 1: Summary of Changes

- This is the first issue of this policy in the updated policy format.