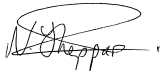




Acceptable Use Agreement

Author:	Josh Collins
Approved By:	Academy Committee
Signature:	
Approval Date:	September 2026
Review Frequency:	Annually
Next Review:	September 2027

1. Introduction

The purpose of this document is to outline the acceptable use of the colleges' Information and Communication Technology platforms, both on and offsite. Guidance for appropriate use and examples of inappropriate use will be referenced but will not be an exhaustive list. This document is intended to protect all parties: students, staff, visitors and anyone given access to the ICT System.

2. Term Definitions

Throughout this document there will be reference of certain terms, their definitions are below:

Staff - An employee of Carisbrooke College

Student - an individual who attends either of the college sites for accessing education

Network User - A user with access to the system infrastructure or core services

Personal Device - A mobile device, such as a laptop or mobile phone, that is not owned by the school

Company Owned Device - A mobile device, such as a laptop or mobile phone, that is owned by the school

Artificial Intelligence (AI) / Generative AI - Systems capable of generating, analysing, transforming, or responding to content/data (e.g., text, images, code, audio).

3. Roles and Responsibilities

The ICT provision is used for a wide range of resources, applications, and access to third-party resources. As a result, responsibilities for the data being accessed are shared between the most appropriate departments and individuals.

The ICT Department will:

Ensure that access to Education based resources is available via a secure and efficient system, whether these resources are held/stored onsite or within cloud-based platforms. Changes to the system and wider network access changes require a review of this, and other ICT related Policies, to ensure they are up to date and accurate at the time of review. The ICT Department is responsible for ensuring staff are aware of their roles and responsibilities with regards to Appropriate Use of the ICT Systems and that all users have evidenced a signed version of this policy before granting access to the system and third-party services. An accurate and efficient overview of the school's web filter is to be maintained, and breaches reported to appropriate Faculty members.

Staff will:

Ensure all guidance within this policy, the Cyber Security Policy and E-Safety Policy are being followed at all times when operating within the ICT System; extended guidance and examples are in the latter part of this document. Staff must ensure students under their supervision are aware of and understand this Policy, have signed this agreement and are familiar with the rules and regulations in place relating to this Acceptable Use Agreement, the Cyber Security Policy and E-Safety Policy. It is the responsibility of the Staff to report any potential breaches of this agreement by colleagues or students to the Service Desk.

Students will:

Adhere to the guidelines specified in this document and understand that breaches of this can result in disciplinary actions and network access being revoked. Ensure that this policy, as part of the New Starter Pack, has been read, understood, signed and returned to their Head of Year before being given access to the network and wider systems in place. Raise concerns regarding potential breaches, either by fellow students, or inappropriate material being accessible to members of the ICT System.

All users will:

Understand that any breaches to the guidelines or attempts to bypass the school's security systems can result in network access being revoked indefinitely, if proven. Agree to the fact that the college reserves the right to examine or delete any files that may be held on its system and related cloud storage platforms, along with monitoring all aspects of live computer use and/or internet sites visited - with or without staff/student permission.

Acceptable use of Computers and Internet Guidance for Staff

Desktop computers on site along with Company Owned Devices are provided for the primary purpose of accessing work related data and applications in a secure manner. The use of such devices are to be used for work related purposes only and the storage of work-related information only, not personal data. Using the college's ICT system for personal and/or private business use is strictly prohibited and the school reserves the right to remove files stored within its on-site or cloud storage platforms that are deemed for personal use. A list of additional guidelines around appropriate and inappropriate use of the system is as follows. Please note, this is not an exhaustive list.

- All computer use, storage and internet activity should be appropriate to the member of staff's employment and is open to scrutiny by IT Support Management and SLT

- Access can only be made via your authorised account and password, using an authorised device
- Your login credentials must not be shared with any other individuals
- Allowing another individual to use a device logged in with your credentials is forbidden
- As per the Cyber Security Policy, passwords must be routinely changed
- Activity that threatens the integrity and security of the ICT system, or activity that attacks/corrupts our/other systems is forbidden, is a criminal offence and will result in disciplinary action
- All communications to parents/students/carers/visitors must be via the school's primary approved systems, such as Google Mail, Arbor or SchoolComms; social media contact is not permitted
- Users are responsible for all emails sent and accept that these will be open to scrutiny
- Access to sensitive data stored within the cloud storage platform(s) must only be accessed via desktop PCs on site or a staff issued company-owned device and authenticated with two Factor authentication. Any attempts to access such data outside of these sources is forbidden
- Use of the system for personal/financial gain is forbidden, as is gambling/betting etc.
- Use of the computer system to access inappropriate materials such as pornographic, racist or other offensive materials is forbidden
- Should you notice, or be made aware of, any concerns or damage to the school infrastructure you are to notify the IT Department via the approved Ticketing Portal as soon as possible
- Staff access to the WiFi is only available using company-owned devices that have been issued to specific staff members and enrolled to a cloud mobile management system, such as Intune or Google's MDM
- All use of college systems, devices, accounts, internet access and communications may be monitored, logged, and reviewed without notice, for safeguarding, security, and operational purposes
- Great care should be taken with giving personal details such as addresses, telephone numbers, bank details etc.
- Personal contact details should never be given out in unregulated situation such as chat rooms
- General Data Protection Regulations (GDPR) and the Computer Misuse Act 1990 apply to all uses of the computers
- If staff are caught misusing the computer network, the school is obliged to act according to the severity of the offence
- Cyberbullying is considered an offence and will result in the same sanctions as other staff bullying incidents
- Any attempts to download, and run, potentially harmful or malicious software will result in action being taken in line with the severity of the attempt
- Programs/software brought in from home and attempting to be installed on the ICT System is not permitted

- USB mass storage devices are not permitted for staff use, data must only be shared within the school's cloud storage platforms and using the chosen services, such as Google Workspace or M365
- Attempting to login with another member of staff's username/password can result in disciplinary action
- Personal devices are not permitted to be joined to the network unless explicitly authorised and vetted in advance, this applies to staff arranging for visitors/speakers to attend the College sites
- Data Protection & Confidentiality: Personal, sensitive, or confidential data (including SEND, safeguarding, medical, or assessment records) must never be entered into unapproved AI tools. Staff must only use platforms listed on the *Approved AI Tools Register*.
- Professional Judgement: AI must never replace professional human judgement or be the sole basis for decisions regarding safeguarding, behavior sanctions, SEND provision, or pupil assessment.
- Accountability & Verification: Staff remain fully accountable for any AI-assisted work, lesson plans, or communications and must verify outputs for accuracy, bias, and appropriateness before use.
- Account Creation: Staff must not require students to create accounts on third-party AI platforms unless explicitly approved by the school.

Staff must have read and understood both the Cyber Security Policy and the E-Safety Policy

This form and agreement must be signed on an annual basis for all members of staff without exception.

I confirm that I have read, understood, and agree to abide by the Carisbrooke College AI Policy alongside this Acceptable Use Agreement.

Full Name:

Signed:

Date:

Acceptable use of Computers and Internet Guidance for Students

Students have access to a number of desktop computers on site, banks of shared mobile devices, individually configured Chromebooks (for specific students) and their personal devices at home. All of these can be used for the purpose of accessing education and school-related data and applications. The use of any company owned device is to be for educational related purposes only and the storage of school/learning related information only, not personal data. Using the ICT system for personal use is strictly prohibited, and the school reserves the right to remove files stored within its on-site or cloud storage platforms that are deemed for personal use. The ICT Department will not take part in any troubleshooting or technician support on a personal device.

A list of additional guidelines around appropriate and inappropriate use of the school's system is as follows. The use of student's own personal devices off-site is not monitored by the school. Please note, this is not an exhaustive list.

- All college owned computer use and internet activity should be appropriate to the student's educational and learning needs
- The organisation will monitor all use of the school systems both locally and cloud hosted
- Access can only be made via your authorised account and password
- Your login credentials must not be shared with any other individuals
- Allowing another individual to use a device logged in with your credentials is forbidden
- Activity that threatens the integrity and security of the ICT system, or activity that attacks/corrupts our/other systems is forbidden and is a criminal offence
- All communications to teachers must be via the school's primary systems, such as Google Mail or Google Classroom, social media contact is not permitted
- All users are responsible for all emails sent and accept that these will be open to scrutiny
- Use of the system for personal/financial gain is forbidden, as is gambling/betting etc.
- Use of the computer system to access inappropriate materials such as pornographic, racist or other offensive materials is forbidden and will result in appropriate sanctions, including internet access being revoked and, if deemed necessary, complete network access being revoked
- Attempts to bypass the school's web filtering system, either successful or unsuccessful, will result in appropriate sanctions
- All use of college systems, devices, accounts, internet access and communications may be monitored, logged, and reviewed without notice, for safeguarding, security, and operational purposes

- General Data Protection Regulations (GDPR) and the Computer Misuse Act 1990 apply to all uses of computers
- If students are caught misusing the computer network, the school is obliged to take action according to the severity of the offence
- Cyberbullying is considered an offence and will result in the same sanctions as other student bullying incidents
- Any attempts to download, and run, potentially harmful or malicious software will result in action being taken in line with the severity of the attempt
- Programs/software brought in from home and attempting to be installed on the ICT System is not permitted
- USB mass storage devices are permitted for specific student level access, such as exams or Creative Arts coursework. This is only an alternative to the primary source of data within the school's cloud storage platforms and using the chosen services, such as Google Workspace or 365
- Attempting to login with another member of student's username/password can result in disciplinary action
- Students must be aware of their role and responsibilities in terms of E-Safety
- This form and agreement must be signed before access will be granted to the ICT system
- Adherence to the AI Framework: Students must strictly adhere to the AI level assigned by their teacher for every task (Level 1: AI Permitted; Level 2: AI Permitted with Restrictions; Level 3: AI Not Permitted; Level 4: Assessed Work/Exam Board Rules). If no level is stated, Level 3 (AI Not Permitted) applies by default.
- Academic Integrity: Presenting AI-generated content as a student's own independent work is prohibited and constitutes academic malpractice.
- Data & Content Restrictions: Students must not upload personal data belonging to themselves or others into AI tools, nor use AI to create harmful, inappropriate, or misleading content, or to impersonate others.

I confirm that I have read, understood, and agree to abide by the Carisbrooke College AI Policy alongside this Acceptable Use Agreement.

Full Name:

Tutor Group:

Year:

Signed [Student]:

Date:

Signed [Parent/Carer]:

Date: