DITCHAM PARK SCHOOL

Where every child is known and valued

Acceptable IT Use Policy - Student

Compiled by	Head of IT
Approved by	Bursar
Date of Publication	September 2018
This Review (Head of IT)	September 2023
Next Review (Head of IT)	September 2024

Acceptable IT Use Policy - Student

1.0 Overview

The School's intentions for publishing an Acceptable IT Use Policy is not to impose restrictions that are contrary to the School's established culture of openness, trust and integrity. Ditcham Park School is committed to protecting the School's staff, students, partners and the charity from illegal or damaging actions by individuals, either knowingly or unknowingly.

Intranet, internet or related cloud-based systems, including but not limited to computer equipment, software, operating systems, storage media as well as network accounts are the property of Ditcham Park School. These systems are also used for business purposes in serving the interests of the School, and any other affiliations pertaining to the school during normal operations.

Effective security is a team effort involving the participation and support of every employee, student or affiliate who deals with information and/or information systems. It is the responsibility of every student to adhere to this Policy, and to conduct their activities accordingly.

The School reserves the right to audit and log all use of laptop/desktop/mobile computers owned by Ditcham Park School for the purpose of ensuring the integrity, security and reliable operation of computer services. Breaches of this Policy will be addressed with appropriate student sanctions as outlined in our Behaviour Rewards and Sanctions Policy.

The School has a statutory duty to take steps to prevent individuals being drawn into extremism and terrorism under The Prevent Strategy of the Counter-Terrorism and Security Act (2015) and a duty to alert and report any attempted access to, or dissemination of, such inappropriate material.

Note: The UK government has defined extremism as: "vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs".

Purpose

This Policy sets out the criteria associated with the acceptable use of the School's Information Technology & Systems and recognises that the security of the systems and the management of risk to assets and users is paramount. These rules are in place to protect both the student and School. Inappropriate use of IT exposes the School to risks including but not limited to virus attacks, compromise of network systems, security and services, and legal issues.

2.0 Scope

This policy applies to students of Ditcham Park School. This policy applies to all equipment that is owned or leased by Ditcham Park School. It also applies to any and all actions on the Internet that inadvertently or intentionally affect Ditcham Park School. Students from other schools or organisations will be expected to abide by the terms of this Policy. Whilst the School will not have the contractual right to take sanctions against this category of student the IT Department or Bursar will have the authorisation to suspend access.

3.0 Policy

4.1 General use and Ownership

1. While Ditcham Park School desires to provide a reasonable level of privacy, users should be aware that the data they create on the School network remains the property of Ditcham Park School. Because of the need to protect the School's network, Senior Leadership Team (SLT) cannot guarantee the confidentiality of information stored on any network device belonging to Ditcham Park School.
2. Ditcham Park School retains the right to monitor and sensor any and all network traffic within the School. This is to ensure the safety, security and reputation of Ditcham Park School.
3. Ditcham Park School reserves the right to audit School equipment on a periodic basis to ensure compliance with this policy.

4.2 Student Chromebook Usage

This section outlines the Schools' expectation for the use of School issued Chromebooks. Your School issued Chromebook remains the property of Ditcham Park School.

I agree that:

- I will bring my Chromebook to school every day, unless otherwise instructed.
- I will come to school with my Chromebook fully charged.
- I will inform the IT Department of any damage immediately.
- I will take every precaution not to damage my Chromebook, this includes: Securing your Chromebook in its' case when not in use, Storing your Chromebook in your school bag when moving between lessons, using your cubby hole outside of lesson time to store your bag/Chromebook.
- I will not touch other pupils' Chromebooks unless instructed by a teacher.
- My Chromebook is a learning tool, it should only be used for, but is not limited to, academic studies and research.

- Any damage that occurs as a result of misuse could result in my parents/guardians being charged.
- I will use my Chromebook in line with the Ditcham Park School 'Acceptable IT Use Policy'.

4.3 Security, GDPR and Proprietary Information

1. Information contained on the intranet, internet or related cloud-based systems should be classified as either confidential or not confidential.
    a. This classification is defined by the Head of IT, GDPR Team or Senior Leadership Team (SLT). Examples of confidential information include but are not limited to: company private, financial, competitor sensitive, specifications, research data, personnel files and student information.
    b. Students should take all necessary steps to prevent unauthorised access to this information.
2. Keep passwords secure and do not share accounts.
    a. Students are responsible for maintaining the security of their own accounts.
3. All students working on any School device should lock their workstation at any time of rest from the device. Alternatively the user should log-off when retired for a long period of time.
4. Because information contained on a students Chromebook or iPad is especially vulnerable, special care should be exercised.
5. Ditcham Park School does not encourage the use of removable media, if students use removable media, such as USB dongles, they shall ensure the device is encrypted and data stored on such devices, is risk free including but not limited to: Viruses, Trojan Horses and other Malware.
6. Postings by students from a School email address to social media/blogs/vblogs is prohibited, unless instructed to by the School.
7. Students must use extreme caution when opening Email attachments or clicking links received from unknown senders, they may contain Viruses, Malware, unknown links, or Trojan Horse codes/links/phishing.
8. Students are not authorised to use the wireless network unless given permission by the IT Department or are using a School supplied device. Use of the wireless network as with the wired network is for professional use only.

4.4 Unacceptable Use

The following activities are, in general, prohibited. Students may be exempted from these restrictions during the course of their time at Ditcham Park School.

Under no circumstances is a student of Ditcham Park School authorised to engage in any activity that is deemed illegal under local, county, national or international law while using School owned resources.

The list below is by no means exhaustive but attempts to provide a framework for activities which fall into the category of unacceptable use.

4.4.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations; Including, but not limited to, the installation or distribution of 'pirated' or other software products that are not appropriately licensed for use by the School.
2. Copying or moving of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources (unless otherwise stated), copyrighted music and the installation of any copyrighted software for which the company, or user does not have an active licence.
3. Exporting software, technical information, encryption software or other technology, in violation of national or international export control laws. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programmes onto the network or servers (e.g. Viruses, Worms, Trojan Horses, Email malware links, etc).
5. Revealing account passwords to others or allowing use of School accounts by others. This includes family and other household members when work is being done at home. Unless instructed to use by the School.
6. Using a School computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
7. Making fraudulent offers of products, items, or services originating from any School account.
8. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the student is not an intended recipient or logging into a server or account that the student is not expressly authorised to access.
    a. For the purposes of these sections, 'disruption' includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service attacks and forged routing of information for malicious purposes.
9. Port scanning or security scanning is expressly prohibited unless prior notification from the IT Department is given.
10. Executing any form of network monitoring which will intercept data not intended for the student.
11. Circumventing user authentication or security of any user account where the user does not have the required authentication rights.
12. Interfering with or denying service to any user (e.g. denial of service attacks).

13. Removing or transferring machine hardware of any description, including, but not limited to, keyboard, mice, headphones and monitors. This is strictly prohibited without the prior authorisation of the IT Department or SLT.
14. Providing information or lists regarding Ditcham Park School teachers or students to parties outside of the School.

4.4.2 Email and Communications Activities

1. Sending unsolicited Email messages, including the sending of 'junk email' or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or messaging, whether through language, frequency, or size of message.
3. Creation or distribution of any disruptive or offensive messages, including but not limited to offensive comments regarding: race, gender, hair colour, disabilities, age, sexual orientation, pornography, religious beliefs and/or practice, political view, or national origin. Students who receive any Emails containing defamatory remarks or comments from another company students must report the matter to any member of staff.
4. Unauthorised use or forging of Email header or footer information.
5. Use of any other Email account to which the user has not been given express permission or rights to use with the intent to harass or collect replies.
6. Creating and forwarding 'chain letters', 'ponzi' or other 'pyramid' type schemes of any kind.
7. Use of unsolicited Email originating from within Ditcham Park School's network, including use of third party Email account originating from other Service Providers, such as, Hotmail, Gmail, Outlook, etc, such use is tolerated by the School, but will still be subject to monitoring; all students except full responsibility for the use of personal, third-party or other company Emailing.

4.5 Blogging (applies to Video Blogging as well)

1. Blogging by students, whether using School property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this policy. Blogging from School systems is also subject to monitoring.
2. Students are prohibited from revealing any School confidential or proprietary information, trade secrets or any other material whilst engaging in blogging.
3. Students shall not engage in any blogging that may harm or tarnish the image, reputations and/or goodwill of Ditcham Park School and/or any of its students/employees. Students are also prohibited from making any discrimination, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by Ditcham Park School.
4. Students may also not attribute personal statements, opinions or beliefs about or pertaining to the School when engaged in blogging. If a student is expressing his or her beliefs and/or opinions in blogs, the student may not, expressly or

implicitly, represent themselves as a student or representative of Ditcham Park School. Students assume any and all risk associated with blogging.
5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled material, the company's trademarks, logo's and any other company intellectual property may also not be used in connection with any blogging activity.

4.6 Online Social Societies (Social Media)

1. The use of online social societies by students, whether using School property and systems or personal computer systems, is prohibited unless otherwise agreed by a member of staff.
2. Students may not, expressly or implicitly, attribute personal statements, opinions or beliefs that can in any way relate to the school.
3. Students may not publish any material that can harm or tarnish the image, reputations and/or goodwill of Ditcham Park School and/or any of its employees. Students are also prohibited from making any discrimination, disparaging, defamatory or harassing comments whilst engaging within online communities.
4. Students may also not attribute personal statements, opinions or beliefs about or pertaining to the company when engaging within online social media. If an student is expressing his or her beliefs and/or opinions, the student may not, expressly or implicitly, represent themselves as a student or representative of Ditcham Park School. Students assume responsibility for any and all risks associated with all forms of online communication.
5. Students are prohibited from revealing any School confidential or proprietary information, trade secrets or any other material whilst engaging in online social societies.

5.0 Monitoring

1. Ditcham Park School students shall have no expectation of privacy in anything they store, send or receive on the School's network.
2. The School may monitor messages without prior notice. The School is not obliged to monitor Email messages unless for training or legal/unlawful purposes.

6.0

Artificial Intelligence (AI)

a. Pupils must prioritize their online safety while using AI, never sharing personal information or engaging in harmful online behaviour.
b. Always use AI tools in a respectful and responsible manner, adhering to school and class codes of conduct.
c. Pupils must not use AI to create or manipulate content with the intention to deceive, including but not limited to falsifying academic assignments, plagiarism, or cheating on tests. Authenticity and honesty in their work are paramount
d. When using AI tools to assist with research or assignments, pupils must cite and reference the AI-generated content appropriately. Plagiarism, even when aided by AI, is not permitted.
e. AI tools should be used for educational purposes as directed by teachers or in alignment with the school curriculum. Pupils should not use AI for unrelated or non-educational tasks during school hours.
f. Pupils should not access AI tools or platforms that have age restrictions or require the sharing of personal information. Always adhere to age-appropriate usage guidelines. Pupils must not engage in activities involving AI that are illegal, harmful, or inappropriate for their age group, including accessing explicit or violent content.
g. Pupils should be aware of the importance of data privacy. They should not share login credentials or access codes for AI platforms with others, and they should report any suspicious activity related to AI tools to a trusted adult, teacher, or parent promptly.

7.0 Enforcement

A student found to have violated this policy may be subject to sanctions in line with the School's Behaviour Rewards and Sanctions Policy.

7.0 Definitions

Term	Definition
Blogging or vBlogging	Writing a blog or video blog. (Short for weblog) is a personal online journal that is frequently updated and intended for public consumption.
Online social society	An online community for people who share interest and activities, or who are interested in exploring the interests and activities of others.
Spam	Unauthorised and/or unsolicited electronic mass mailings
Email	The electronic transmission of information through a mail protocol such as SMTP or IMAP. Typical Email clients include Eudora and Microsoft Outlook.
Forward Email	Email resent from an internal network to an outside point.
Chain mail or letter	Email sent to successive people. Typically the body of the note has direction to send out multiple copies of the note and promises good luck or money if the direction is followed.
Sensitive information	Information considered sensitive if it can be damaging to the company's reputation or market standing.