DITCHAM PARK SCHOOL

Where every child is known and valued

Acceptable Computer Use Policy

Compiled by	Head of IT
Approved by	Bursar
Date of Publication	September 2018
Next Review	September 2019

Acceptable Computer Use Policy

1.0 Overview

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

Internet/Intranet/Extranet-related or cloud based systems, including but not limited to computer equipment, software, Operating Systems, storage media, network accounts both providing and denying electronic mail, WWW browsing and FTP are the property of Ditcham Park School. These systems are also used for business purposes in serving the interests of the company, 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 employee to know these guidelines, and to conduct their activities accordingly.

The School reserves the right to audit and log all use of laptop/desktop/mobile computers for the purpose of ensuring the integrity, security and reliable operation of computer services. Breaches of this Policy will be treated as a disciplinary matter.

The School has a statutory duty to take steps to prevent individuals being drawn into extremism and terrorism under the PREVENT element 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.

2.0 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 employee and company. Inappropriate use of ICT exposes the company to risks including but not limited to virus attacks, compromise of network systems, security and services, and legal issues.

3.0 Scope

Acceptable Computer Use Policy

This policy applies to consultants, contractors, employees, students, temporary staff and other workers at Ditcham Park School, including all personnel affiliated with third-party companies.
This policy applies to all equipment that is owned or leased by the company. It also applies to any and all actions on the Internet that inadvertently or intentionally affect the company.
Staff from other organisations will be expected to abide by the terms of this Policy. Whilst the School will not have the contractual right to take disciplinary action against this category of staff the Head of IT or Bursar will have the authorisation to suspend access.

4.0 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 corporate network remains the property of the company. Because of the need to protect the company's network, management cannot guarantee the confidentiality of information stored on any network device belonging to the company.
2. The company retains the right to monitor and sensor any and all network traffic within the company. This is to ensure the safety, security and reputation of Ditcham Park School.
3. The company reserves the right to audit company equipment on a periodic basis to ensure compliance with this policy.

4.2 Security, GDPR and Proprietary Information

1. Information contained on the Internet/Intranet/Extranet should be classified as either confidential or not confidential. The School takes its compliance with the General Data Protection Regulation (**GDPR**) seriously and aims at all times to keep personal data secure. It takes suitable measures to prevent unauthorised or unlawful processing of personal data and accidental loss or destruction of or damage to personal data. All members of School Staff and Governors are required to undertake **GDPR** training provided by the School. The training provided is designed to help Staff understand key areas of compliance and to provide evidence that staff have read and understood relevant policies and documents.
    a. This classification is defined by the Head of IT, **GDPR** Team or Senior Leadership Team. Examples of confidential information include but are not limited to: company private, financial, competitor sensitive, specifications, research data, personnel files and student information.
    b. Employees should take all necessary steps to prevent unauthorised access to this information as outlined through **GDPR** training and GDPR documentation.
2. Keep passwords secure and do not share accounts.

   a. Users are responsible for maintaining the security of their own accounts. System or high confidentiality level passwords should be changed each academic year; User level passwords should invoke best practice and be changed every academic year, though this is not required.
3. All staff members at machines should lock workstations at any time of rest from the machine, alternatively the user should log-off when retired for a long period of time.
4. Because information contained on portable computers (laptops) or mobile devices is especially vulnerable, special care should be exercised.
5. The School does not encourage the use of USB memory sticks or any other removable media by Employees which may be easily mislaid. If the Employee needs to use them it must be with the permission of the Chief Privacy Officer and/or the Head of IT and only when the USB memory stick or removable device has been encrypted and password protected.
6. Postings by employees from a company Email address to newsgroups/social media/blogs/vblogs should contain a disclaimer stating the opinions expressed are strictly their own and not necessarily those of the company, unless posting is in the course of business duties.
7. All machines used by employees that are connected to the company Internet/Intranet/Extranet, whether owned by the employee or company shall be continually executing approved anti-virus software with an up-to-date virus database, unless overridden by IT support or Group Policy.
8. Employees must use extreme caution when opening Email attachments received from unknown senders, they may contain Viruses, Malware, unknown links, Email bombs, or Trojan Horse codes/links.
9. The use of the schools wireless network (Wi-Fi) for use on wireless devices such as mobile phones, PDA's, laptops, tablet computers or any other device with the ability to access the wireless network is governed under the same rules and policies as the wired network. Staff may access the wireless network providing they have been given authorisation by the ICT Department. Students are not authorised to use the wireless network unless given permission by the ICT Department. Use of the wireless network as with the wired network is for professional use only.

4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g. system administration staff may require the need to disable network access of a user if their actions disrupt normal operations).
Under no circumstances is an employee of Ditcham Park School authorised to engage in any activity that is deemed illegal under local, county, national or international law while using company 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.

4.3.1 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 company.
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 server (e.g. Viruses, Worms, Trojan Horses, Email malware links, etc).
5. Revealing account passwords to others or allowing use of company accounts by others. This includes family and other household members when work is being done at home.
6. Using a company 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 company account.
8. Making statements about warranty, expressly or implied, unless it is part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorised to access, unless these actions are within the scope of regular duties.
    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.
10. Port scanning or security scanning is expressly prohibited unless prior notification from the IT Department is given.
11. Executing any form of network monitoring which will intercept data not intended for the employee, unless this activity is a part of the employee's duties.
12. Circumventing user authentication or security of any user account where the user does not have the required authentication rights.
13. Interfering with or denying service to any user (e.g. denial of service attacks).
14. 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.

15. Providing information or lists regarding Ditcham Park School employees or students to parties outside of the company.

4.3.2 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 paging, 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. Employees who receive any Emails containing defamatory remarks or comments from another company employee must report the matter to a member of the IT Department, their Line Manager or Senior Leadership Team team immediately.
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, Google Mail, AOL, etc, such use is tolerated by the company, but will still be subject to monitoring; all employees except full responsibility for the use of personal, third-party or other company Emailing. Advertisement of any service hosted by the company or connected via the company's network is also strictly prohibited.
8. Posting the same or similar non-business-related messages to large numbers of use internet newsgroups (newsgroup spam).

4.4 Blogging (applies to Video Blogging as well)

1. Blogging by employees, whether using company property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this policy. Limited and occasional use of Ditcham Park School's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate the company's policy, is not detrimental to the company's best interests, and does not interfere

with an employee's regular working duties. Blogging from company systems is also subject to monitoring.
2. Employees are prohibited from revealing any company confidential or proprietary information, trade secrets or any other material whilst engaging in blogging.
3. Employees 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 employees. Employees 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. Employees may also not attribute personal statements, opinions or beliefs about or pertaining to the company when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Ditcham Park School. Employees 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.

4.5 Online Social Societies (Social Media) (also see Social Media Policy)

1. The use of online social societies by employees, whether using company property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this policy. Limited and occasional use of Ditcham Park School's systems to engage in online communities is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate the company's policy, is not detrimental to the company's best interests, and does not interfere with an employee's regular working duties. Use of online social media from company systems is also subject to monitoring.
2. Employees may not, expressly or implicitly, attribute personal statements, opinions or beliefs that can in any way relate to the company.
3. Employees 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. Employees are also prohibited from making any discrimination, disparaging, defamatory or harassing comments whilst engaging within online communities.
4. Employees may also not attribute personal statements, opinions or beliefs about or pertaining to the company when engaging within online social media. If an employee is expressing his or her beliefs and/or opinions, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Ditcham Park School. Employees assume any and all risks associated with all forms of online communication.
5. Employees must also exert and uphold professional conduct whilst engaging in online communities, the ability to form friendships and/or ties with current and past students within online communities must be undertaken with extreme care,

under no circumstances should an employee engage in activities that may bring the school into disrepute, this includes any and all actions available within an online social society.

6. Employees are prohibited from revealing any company confidential or proprietary information, trade secrets or any other material whilst engaging in online social societies.

5.0 Monitoring

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

6.0 Enforcement

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Compiled by Mat Mitas	Date: September 2018
Approved by Bursar	Review Date: September 2019

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.