OAKLANDS COLLEGE

# IT Security policy

## 1. Overview

IT Solutions intentions for publishing a Staff IT Security Policy are not to impose restrictions that are contrary to Oaklands established culture of openness, trust, and integrity. IT Solutions is committed to protecting Oaklands employees, partners, and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and VPN, are the property of Oaklands. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers during normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every Oaklands employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

## 2. Purpose

The purpose of this policy is to outline the secure use of all IT systems at Oaklands. These rules are in place to protect the employee and Oaklands. Inappropriate use exposes Oaklands to risks including virus attacks, compromise of network systems and services, and legal issues.

## 3. Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Oaklands business or interact with internal networks and business systems, whether owned or leased by Oaklands, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at Oaklands and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Oaklands policies and standards, and local laws and regulation. Exceptions to this policy are documented in section 5.2

This policy applies to employees, contractors, consultants, temporaries, and other workers at Oaklands, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Oaklands.

## 4. Policy

### 4.1 General Information Protection

4.1.1 Oaklands proprietary information stored on electronic and computing devices whether owned or leased by Oaklands, the employee or a third party, remains the sole property of Oaklands. You must ensure through legal or technical means that proprietary information is protected in accordance with the Data Protection Act and GDPR.

4.1.2 You have a responsibility to promptly report the theft, loss, or unauthorized disclosure of Oaklands proprietary information.

4.1.3 You may access, use or share Oaklands proprietary information only to the extent it is authorized and necessary to fulfil your assigned job duties.

4.1.4 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guideline concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

4.1.5 For security and network maintenance purposes, authorized individuals within may monitor equipment, systems, and network traffic at any time.

4.1.6 reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

### 4.2 Security and Proprietary Information

4.2.1 All mobile and computing devices that connect to the internal network must comply with the Minimum Requirements for Network Access (Section 4.5).

4.2.2 System level and user level passwords must comply with Section 4.4 (Password Construction, Use and Protection). Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

4.2.3 All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

4.2.4 Postings by employees from an Oaklands email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Oaklands, unless posting is during business duties.

4.2.5 Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

### 4.3 Unacceptable Use

#### 4.3.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

4.3.1.1 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 Oaklands.

4.3.1.2 Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Oaklands or the end user does not have an active license is strictly prohibited.

4.3.1.3 Accessing data, a server, or an account for any purpose other than conducting Oaklands business, even if you have authorized access, is prohibited.

4.3.1.4 Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

4.3.1.5 Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

4.3.1.6 Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

4.3.1.7 Making fraudulent offers of products, items, or services originating from any account.

4.3.1.8 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 authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

4.3.1.9 Port scanning or security scanning is expressly prohibited unless prior notification to IT Support is made.

4.3.1.10 Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

4.3.1.11 Circumventing user authentication or security of any host, network, or account.

4.3.1.12 Introducing honeypots, honeynets, or similar technology on the Oaklands network.

4.3.1.13 Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

4.3.1.14 Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

4.3.1.15 Providing information about Oaklands, or lists of, Oaklands employees to parties outside.

### 4.3.2 Email and Communication Activities

When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the IT Department

4.3.2.1 Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

4.3.2.2 Any form of harassment via email, telephone, or paging, whether through language, frequency, or size of messages.

4.3.2.3 Unauthorized use, or forging, of email header information.

4.3.2.4 Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

4.3.2.5 Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

4.3.2.6 Use of unsolicited email originating from within Oaklands networks of other Internet/Intranet/Extranet service providers on behalf of Oaklands, or to advertise, any service hosted by or connected via Oaklands network.

4.3.2.7 Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

### 4.3.3 Blogging and Social Media

4.3.3.1 Blogging by employees, whether using Oaklands 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 Oaklands systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Oaklands policy, is not detrimental to Oaklands best interests, and does not interfere with an employee's regular work duties. Blogging from Oaklands systems is also subject to monitoring.

4.3.3.2 Oaklands Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any confidential or proprietary information, trade secrets or any other material covered by Oaklands Confidential Information policy when engaged in blogging.

4.3.3.3 Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of Oaklands and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by Oaklands Non-Discrimination and Anti-Harassment policy.

4.3.3.4 Employees may also not attribute personal statements, opinions, or beliefs to Oaklands 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 Oaklands. Employees assume any and all risk associated with blogging.

4.3.3.5 Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, Oaklands trademarks, logos and any other Oaklands intellectual property may also not be used in connection with any blogging activity.

## 4.4 Password Construction, Use and Protection

Passwords are a critical component of information security. Passwords serve to protect user accounts; however, a poorly constructed password may result in the compromise of individual systems, data, or the Oaklands network. This guideline provides best practices for creating secure passwords.

### 4.4.1 All passwords must meet or exceed the following strength guidelines.

**Strong passwords have the following characteristics:**

4.4.1.1 Contain at least 12 alphanumeric characters.

4.4.1.2 Contain both upper and lower case letters.

4.4.1.3 Contain at least one number (for example, 0-9).

4.4.1.4 Contain at least one special character (for example,!$%^&*()_+|~-=\`{}[]:";'<>?,/).

### 4.4.2 All passwords should not have any of the following characteristics:

4.4.2.1 Contain less than twelve characters.

4.4.2.2 Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.

4.4.2.3 Contain personal information such as birthdates, addresses, phone numbers, or names

4.4.2.4 of family members, pets, friends, and fantasy characters.

4.4.2.5 Contain work-related information such as building names, system commands, sites, companies, hardware, or software.

4.4.2.6 Contain number patterns such as *aaabbb*, *qwerty*, *zyxwvuts*, or *123321*.

4.4.2.7 Contain common words spelled backward, or preceded or followed by a number (for example, *terces*, *secret1* or *1secret*).

4.4.2.8 Are some version of "*Welcome123*" "*Password123*" "*Changeme123*"

### 4.4.3 You must never write down a password.

Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R! or another variation. (NOTE: Do not use either of these examples as passwords!)

### 4.5 Minimum Access Requirements for Network Connected Devices

4.5.1 **All devices connected to the internal 'local.oaklands.ac.uk' or 'Oaklands' Networks must comply with the following standards:**

4.5.1.1 The device must be securely erased and provisioned with Oaklands approved software and operating system.

4.5.1.2 IT Solutions must fully manage the device.

4.5.1.3 No end user will have administrative access at any level to the device.

4.5.1.4 The user's corporate login username and password must be used to access the device.

4.5.1.5 Installation and execution of any software without explicit permission from IT Services is strictly prohibited.

4.5.1.6 Uninstallation, Circumvention, or bypass of management methods within the device is strictly prohibited.

4.5.1.7 Antivirus and Antimalware software must be installed, activated and have a minimum patch level of 2020Q4.

### 4.6 Incident Reporting

4.6.1 Security breaches at Oaklands are reported along a chain depending on who is notified first and depending on the scope of the breach. The breach should first be reported to the servicedesk@oaklands.ac.uk, where they can notify the relevant parties of the breach and perform a damage assessment. This is then passed to the Senior IT engineers and Head of IT to contain the breach if necessary and minimise business impact. If personal data was breached, the matter is then passed to the data protection officer of the college.

## 5. Policy Compliance

### 5.1 Compliance Measurement

The IT Solutions team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

### 5.2 Exceptions

Any exception to the policy must be approved by the IT Solutions team in advance.

### 5.3 Non-Compliance

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

## 6. Related Standards, Policies, and Processes

Acceptable use policy
e-Safety Policy
BYOD Policy
Social Media and E-safety Policy

## 7. Definitions and Terms

Please see https://www.sans.org/security-resources/glossary-of-terms/ For an explanation of any terms in this document that you may not understand or know of.