# ISMS 004 - Acceptable use – Student

## Acceptable Use – Student summary

Oaklands College provides IT facilities to enable and enhance the College's educational and operational activities for its community of students and staff. This acceptable use policy is a set of rules applied by the Head of IT that restricts the ways in which the Oaklands College Network may be used in order to ensure the safety and security of the network, the information assets held therein and its users.

### SCOPE

This Policy applies to students, who wish to use the College's IT facilities. This acceptable use policy also applies to anyone using their own personal device such as a laptop, tablet or smart phone connected to the Oaklands College Network via WIFI or a wired connection.

### PURPOSE

This Policy defines acceptable and unacceptable behaviours for use of the College's IT and communications facilities and the consequences of unacceptable conduct in order to keep users and information safe from harm.

### RESPONSIBILITY

It is the responsibility of the user to understand this policy and apply its rules to their working practices as a student or other associated person.

### SAFEGUARDING

### KEEPING YOURSELF AND OTHERS SAFE

The Internet is full of useful sites but can be a dangerous place. You can endanger your own information and that of others by replying to emails from people you do not know or giving someone, you do not know personal details (especially on Social Networking sites).

You should never give someone else personal information, including your User ID or password on any system (including ours). Email may well appear to come from someone you know but actually be from someone else. Oaklands staff will never ask for your password by email although we may have to change it for operational reasons (and we will inform you if this is the case).
To be read in conjunction with the following policies

- Social media and E-safety policy
- BYOD Policy
- IT Security Policy
- Safeguarding policy
- Student bullying and Harasment policy
- Student behaviour policy

# ISMS 004 - Acceptable use – Student

## PREVENT DUTY

The college has a duty placed upon it from the section 21 of the Counter-Terrorism and Security Act 2015 to "need to prevent people from being drawn into terrorism." Therefore, any staff or student making use of Oaklands College IT facilities may have their activity monitored to this end, however this does not mean that staff, students or communities of particular religious beliefs will be singled out for monitoring.

Any students who have concerns about the potential radicalisation of fellow colleagues or students using the College's IT systems and networks to communicate or access information that has the potential to radicalise; should contact a safeguarding officer to report their concerns to be dealt with. This is irrespective of if they are using their own or the college's computing facilities. This also includes staff or students posting on social media (inside or outside the college) materials to radicalise, or if they are signed up to receive such communications; to report this to a College safeguarding officer.

The principles of the Prevent Duty fall within the College's obligations around Safeguarding, any communications via the Internet will be monitored and potentially offensive or nefarious websites or materials blocked, any sites that staff or students find that raise concerns that are accessible should be reported to the Oaklands College service desk by emailing servicedesk@oaklands.ac.uk to be blocked.

## RULES

### DO

- Keep your User ID and password safe.
- Always lock (hold the 'Windows' key down and press the 'L' key) or log off from a computer if you leave it (even for a minute) and log-off if you are leaving a terminal for a long period of time in case someone else wants to use it.
- Look after equipment you are using and use any security facilities provided.
- Tell us if there are problems or equipment has been lost or stolen.
- Tell us if you think you or someone else has access to something you/they shouldn't or you think a breach of security of the college's information has or is about to happen.
- If you are using your own equipment on our network, make sure it is checked for viruses and has the latest windows updates applied.
- Contact us on servicedesk@oaklands.ac.uk or by calling the service desk by phone.

### DO NOT

- Use anyone else's account but your own.
- Send email or access information using someone else's identity.
- Use your College email address for personal communications.
- Send personal information in relation to Oaklands staff or students unencrypted to any 3rd party.
- Attempt to access or transmit information about other people's accounts or private information.
- Give your password to ANYONE else (this includes IT Solutions staff).
- Open, respond to or forward unsolicited mails or open any unknown attachments.
- Attempt to access (hack into) systems to which you don't have authorisation.
- Use file sharing or torrent software on our systems.
- Make copies of copyrighted material (DVDs, CDs or other copyrighted media).
- Install software on College computers without the agreement of servicedesk@oaklands.ac.uk
- Take or send personal data or other information about identifiable members of the College community off site or communicate it to others.
- Engage in activities which might deny or disrupt access for others.
- Spend time on social networking sites when you should be working.
- Vandalise, damage or perform repairs on any college equipment
- Remove any college equipment off Campus

- Remove cables from computers (e.g. power cables or network cables) – Unless with consent of IT Solutions staff. If you find there is a room without sufficient network or power points notify the "Servicedesk".
- Send "Spam" or "bulk marketing" emails from your college email account, whether they are relevant to college operations or not. The Marketing department can advise on the use of e-mail for marketing purposes.

### BANNED MATERIAL AND ACTIONS

You must not access, display, store, distribute, use or create using the Oaklands College computing facilities and networks by use of internal processing facilities or external cloud based processing facilities such as social media networks or cloud services:

- Offensive, obscene or indecent material
- Viruses or material designed to create viruses
- Hacking tools
- Material which is:
    - designed to bully  threaten, harass, annoy, inconvenience or cause anxiety to others
    - of a politically extreme or racist nature
    - contravenes the College's Equality Agenda
    - defamatory
    - designed to defraud
    - otherwise illegal
    - which might bring the College into disrepute

This includes material created outside the College - for example a Facebook page abusing a teacher or student.

You should remember that content you find amusing might constitute harassment or offence to another recipient or observer on the grounds of sex, race, disability, religion, belief, sexual orientation, age or taste.

### CONSEQUENCES

If you break the conditions of this Policy, you may be subject to disciplinary action under the College's Student Behaviour Policy and Procedure

A serious breach of the Policy may be treated as Gross Misconduct. Perpetrators of illegal activity on the Oaklands College Network will be reported to the relevant authorities.