OAKLANDS COLLEGE

ACCEPTABLE USE POLICY - Staff

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 (AUP) 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 staff, stakeholders, contractors, associates, and visitors to the College 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 WI-FI 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 staff member, stakeholder or other associated person.

1. MONITORING

The College reserves the right to monitor usage of its computing facilities, in order to ensure optimum performance and proper use in accordance with this policy. The allocation of a user ID and password to access the College's computer network does not imply any right to privacy. Such monitoring may be undertaken randomly or at fixed period's dependent upon the computing facility. All users should be aware that the use of the College's Internet and Intranet provision is monitored and a log of all transactions involving Internet access is available.

You should be aware that all the data stored on and transmitted to and from our systems is liable to be included as part of the monitoring. This monitoring can also include emails, messaging, web traffic and documents saved and transmitted. This monitoring is to ensure that the College runs efficiently and that this AUP is complied with. Normally this means that we only examine data and traffic volumes and not the content of individual items: however, our automated monitoring systems do examine content to determine whether emails, messages, data or web sites breach the conditions of this AUP or come from sources of known nuisance or malicious intent, this monitoring will comply with the Telecommunications (Lawful Business Practice)(Interception of

Communications) Regulations 2000 ("LBP Regulations") and Regulation of Investigatory Powers Act 2000 ("RIPA") laws and legislation.

If we have reasonable grounds for believing a crime or breach of the College's Policies has been committed by you (or we have had complaints from staff, students or external parties about your conduct or actions), we may access your personal information stored on or transmitted through our systems as part of any investigation and provide it to the relevant authorities or to supply information to any disciplinary procedures. Note: that due procedure will be followed and additional access procedures followed to request access to information formally will be used.

Monitoring of computer use does not extend to viewing e-mail messages created by individual users unless the user's consent has first been sought. However, if a user has requested technical assistance from the service desk to access e-mails, such consent is deemed to have been given. Where obtaining such consent is not practicable or appropriate, (e.g. where misconduct is reasonably suspected), the express written permission of the Vice Principal of HR or the HR manager must be obtained. If access is granted, the user will be informed of the action which has been taken. Where managers use a computer file, e-mail message or computer log of user actions to investigate a suspected abuse, it will be disclosable if relevant to legal or disciplinary proceedings.

It may be necessary, due to sickness, holiday or other reasons, for the College to check staff email and data areas for business continuity and operational reasons.

For access to staff email, data areas or internet usage, managers must put a request in writing to the Vice Principal of HR or the HR manager, specifying why they require access. The Vice Principal of HR or the HR manager will then assess the request and either approve or decline. If approved the Vice Principal of HR or the HR manager will contact the Head of IT who will then provide the manager with access.

Staff who have been absent from work due to sickness or annual leave will be informed that their manager has been given access upon their return to work. For investigation purposes, the College reserves the right to monitor employees' email, data areas and internet usage, but will endeavour to inform an affected employee when this is to happen and the reasons for it.

2. POSSESSION, ACCESS, AND OWNERSHIP OF COLLEGE IT EQUIPMENT

All staff or students who have in their possession an item of College owned IT equipment (e.g. Laptop, Mobile Telephone etc.) must when requested by a member of the IT Solutions team staff return it to a campus IT Solutions office as soon as possible. Repeated (and unjustifiable) failures to return equipment when requested may mean the member of staff or student are subject to disciplinary action.
All IT equipment is owned by the college. Departments, teams, staff and students are granted access by the College to use it. No department, team, member of staff or student 'owns" any equipment provided by the College via the IT Solutions team.

Deliberate impeding access to computing resources by a department, team or member of staff is not acceptable behaviour and that member of staff may face disciplinary action.

3. ACCEPTABLE USE

3.1 Oaklands College's computer network Internet and Intranet provision may be used by staff, enrolled students and external guests (where appropriate) for any legal activity that is in furtherance of the aims and policies of the College. However, all usage must be carefully managed to ensure that the College's image and reputation is properly protected; its liability limited; its data security maintained; usage is for legitimate purposes only and is accomplished in a cost-effective manner.

3.2 This policy must be read in conjunction with the following:

- BYOD Policy
- Social Media and E-Safety Policy
- IT Security Policy
- Professional standards policy

4. UNACCEPTABLE USE

4.1 Users must not cause any form of damage to the College's computing equipment or software, nor to any of the rooms and their facilities and services which contain that equipment or software. The term "damage" includes modifications to hardware or software which, whilst not permanently harming the hardware or software, incurs time and/or cost in restoring the system to its original state. Costs associated with repairing or replacing damaged equipment or software and/or in providing temporary replacements may be charged to the person or persons causing the damage. The costs will be determined by the designated authority.

4.2 The College network Internet and Intranet services may **not** be used for any of the following:

- The creation or transmission (other than for properly supervised and lawful research purposes) of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;
- The creation or transmission of material which is designed or likely to cause harassment, annoyance, inconvenience or needless anxiety;
- The creation or transmission of defamatory material;
- The connection of any device into the College's computer network without prior agreement from an appropriate designated authority;
- The unauthorised purchase of "goods" and/or "services" through the Colleges network and/or Internet services;
- The transmission of material such that this infringes the copyright of another person;
- The sharing or documenting of Logins and/or passwords;
- The transmission of unsolicited commercial or advertising material either to other User Organisations, or to organisations connected to other networks, save where that material is embedded within, or is otherwise part of, a service to which the member of the User Organisation has chosen to subscribe;
- Deliberate unauthorised access to facilities or services accessible via the college's computer network or Internet provision;

4.3 Deliberate activities with any of the following characteristics are **not** permitted:

- Wasting staff effort or networked resources, including time on end systems accessible via the Colleges' computer network, Internet and/or Intranet facilities and the effort of staff involved in the support of those systems;
- Corrupting or destroying other users' data;
- Violating the privacy of other users;
- Disrupting the work of other users;
- Using the College's computer network, Internet and/or Intranet service in a way that denies service to other users (for example, deliberate or reckless overloading of access links or of network equipment);
- Continuing to use an item of networking software or hardware after an appropriate designated authority has requested that use cease because it is causing disruption to the correct functioning of the College's computer network, Internet or Intranet provision;
- Other misuse of the College's computer network and/or networked resources, such as the introduction of "Viruses", "Worms", "Trojan Horses" or other programs which have a 'harmful' or nuisance affect.
- The taking of deliberate action to circumvent any precautions taken by the College to safeguard the security of its computer systems.
- 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.

4.4 Where the College's network, Internet or Intranet facility is being used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of the College's computer network, Internet and/or Intranet services.

4.5 The use of any of the College's computing facilities for commercial gain, for work on behalf of others or for private or personal use (unconnected with a student's course of study at the College or a member of staff's legitimate activities) is not permitted, unless prior agreement has been made with the designated authority for the facilities and an appropriate charge for that use has been determined.

5. Security & Confidentiality

The College holds a significant amount of data that is sensitive in nature, it is the responsibility of any user of the system to comply with the College's "Information Security Policy" and not divulge information to unauthorised parties, act in such a way that allows unauthorised parties access to the data act. The IT Solutions department won't be held responsible for loss of information on a computer that was left unlocked and unattended for long periods of time.

All users (staff, students or contractors) should ensure their computer terminal is locked if they are to leave it for short periods of time. The lock must require that the user be prompted for the username and password before they are allowed access.

If you are leaving your terminal for a long period of time you should log-off the terminal this is especially required in communal computing areas, your terminal may be logged off for you and you may lose your work if you do not do so at the end of your session.

To ensure that you do not disclose information to unauthorised parties you should follow this guidance when dealing with a request for personal or sensitive information from an internal or external party:

Ensure suitable identification has been produced by the individual requesting the information:

- For staff this would be a valid staff badge, their identity should be confirmed by consulting the college's student record system to verify the staff identity.
- For external parties, the only external party we are obliged to provide information to are the law enforcement services, but again do so once shown suitable identification.
- Any other external parties that are requesting sensitive or personal information to be referred to the college data controller to make a formal information request.
- For students requesting their information this may be done so after verifying their student ID badge and identity with their student record within the student information system.
- For requests via the telephone internally it is recommended that the requesting person are challenged by asking them to identify themselves by providing information that only they would know.
- For requests via the telephone externally, staff should not provide personal information about a member of staff or student at all, but instead ask them to make the request in writing via email to the college data controller.
- You should also "sanity check" any request for validity, ask yourself questions like "why are they asking for this information?", if you cannot see a valid reason why the requestor would need the information you should reject the request.

5.1 User passwords must be kept confidential and are not to be disclosed except to the IT Solutions department to enable work to be carried out. With this one exception, it is not acceptable to share passwords with colleagues.

5.2 All users are responsible for ensuring that they do not introduce viruses into the College's computer network. Initial protection must be secured by ensuring that virus check software is installed and upgrades run as available. In particular, the source of all e-mail attachments must be verified prior to opening the attachment. The advice of the IT Solutions department via the Servicedesk must be obtained and followed with reference to any e-mail attachment of uncertain origin or content.

5.3 Data which is of a highly sensitive or confidential nature should not be sent by e-mail as there is a high risk that it will reach or be accessed by inappropriate recipients.

5.4 Users should be aware that data is not normally deleted from a computer's hard disk when an instruction to delete a file, e-mail or other record is executed. The assistance of the IT Solutions department should be sought if any machine, which has been used for storing highly sensitive data, is to be relocated or decommissioned.

WHERE TO STORE INFORMATION SECURELY

The storage of information is difficult to control however as a member of staff (or student), you are the guardian of your or your departments data and are obliged to keep it safe. Therefore, you should store college information in the following locations only:

- One Drive as part of your Microsoft 365 access
- SharePoint online in document libraries
- Teams
- E-Mail Mailbox

If you store information outside of these locations it is at risk of loss, IT Solutions will not be held responsible for data that is lost if it is not stored in the locations as stated above which are protected by the College's backup infrastructure.

These locations are backed up (based on the College's backup schedule), and therefore can be recovered (in accordance with the IT Solutions SLA.)

Do not store College information on the local hard disk (C: Drive) of your desktop or laptop computer, it will not be recoverable if lost and may be inadvertently destroyed if the machine is re-built or components replaced.

A USB Stick or USB external hard drive is not a long-term storage medium for the College's data (due to the high risk of loss or corruption), you should only use this for the transporting information from place to another and should keep at least one additional copy in the locations stated above, i.e. this should not be your primary storage location for data.

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 harassment policy

STAFF – REMOTE LEARNING

Where education is taking place remotely for example due to coronavirus (COVID-19), it is important that colleges maintain professional practice as much as possible. When communicating online with parents, carers, and students, colleges should:

- Communicate within college hours as much as possible (or hours agreed with the college to suit the needs of staff)
- Communicate through the college channels approved by the senior leadership team
- Use college email accounts (not personal ones)
- Use college devices over personal devices wherever possible
- Advise staff not to share personal information
- Ensure parents and carers are clear when and how they can communicate with teachers (resources to support communications are available)
- Ensure logins and passwords are secure and students understand that they should not share this information with others
- Microsoft teams in Office 365 is the default choice for remote learning platform
- Microsoft Teams within Office 365 - to **stop students rejoining a Teams call without the teacher**, you must click End Meeting, not the classic 'hang up' button.

Teachers should try to find a quiet or private room or area to talk to students, parents or carers. When broadcasting a lesson or making a recording, consider what will be in the background

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 staff or 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.

PROTOCOLS FOR CONTACTING STUDENTS

From time to time you may need to contact students. It is always preferable to use Teams to make a call to a student or a colleague, or use other mechanisms such as student email accounts or the student ILP to communicate with students. Should you need to make a call to a student using your personal phone, you should hide your caller ID either using the 141 prefix before the student's telephone number or hiding your caller ID through the settings menu on your mobile phone so as to avoid sharing your personal mobile telephone number with students. Where possible, these types of calls should be kept to a minimum and take place at a mutually agreed time. Staff should not give their personal contact details to students for example, e-mail address, home or mobile telephone numbers or any details of web-based identities. If students locate these by any other means and attempt to contact or correspond with the you, please do not respond and report this to your manager.

6. PERSONAL RESPONSIBILITY

6.1 It is essential that the provisions of this policy are understood and observed by the whole College Community. If anyone is not clear about any of the rules it is their responsibility to seek advice and ask for further guidance. If anyone is aware of actions which do not comply with this policy or they are affected by actions which are not permitted, they should retain any evidence (e.g. copy of an e-mail message, document) and report the matter to a member of staff or line manager as appropriate.

7. ENFORCEMENT

7.1 Failure to comply with this policy may result in withdrawal of access to IT facilities, local, College-wide or external, at the discretion of the Head(s) of the Department(s) concerned. It may also result in further investigation and invoking of the College's formal disciplinary procedures. Infringement of certain regulations may be subject to penalties under civil or criminal law and such law may be invoked by the College.

8. CONSEQUENCES

If you break the conditions of this Policy, you may be subject to disciplinary action under the College's:

- Disciplinary, Capability and Grievance Policy (for staff)
- Student Behaviour Policy and Procedure
- Safeguarding policy
- Student bullying and harassment policy
- Professional standards policy

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.