OAKLANDS COLLEGE

Social media and E-safety policy – Staff

1. Introduction

1.1 Oaklands college is dedicated to promoting our values of honesty, integrity, mutual respect and personal accountability to support our students in becoming fully rounded members of society with a strong sense of social and moral responsibility. We prepare our students for life in Modern Britain by developing an understanding of democracy, the rule of law, individual liberty, mutual respect and tolerance of those with different faiths and beliefs and this is reflected in our policies.

1.2 The College recognises the legitimate role that social media has in both the educational work of the College and in communicating its services. It also acknowledges the value social media can add to our business if used in a responsible and professional way. The College is always committed to maintaining confidentiality and professionalism whilst also upholding its reputation so has an expectation that employees using social media will exhibit appropriate conduct in ways that are consistent with College values and policies.

1.3 This policy outlines the responsibilities of all employees of the College when using social media either personally or for College purposes, to manage organisational risks relating to social media use and to ensure that such use does not bring the College into disrepute.

1.4 This policy should be read in conjunction with the following:

- Bring Your Own Device Policy
- IT Security Policy
- Acceptable Use Policy

2. Definitions and Scope

2.1 Social media is a term used to describe the online tools, websites and interactive media that enable users to share information, opinions, knowledge, and interests. Social media involves building online communities or networks, which encourage participation, dialogue, and comment. Social networking applications include, but are not limited to: blogs, online discussion forums, social and business networking, wikis, social bookmarking and tagging, photo and video sharing, and games that create virtual worlds. Examples of popular social media platforms include Facebook, Twitter, LinkedIn, and YouTube.

2.2 E-Safety is a term used to describe techniques and procedures for being safe online, using common sense, technical measures, and keeping an open mind to online scams, fraud, malicious sites, and being weary of dangerous people on the internet.

2.3 This policy applies to all social media applications, including those currently in existence and any new platforms that may appear in the future. It also applies to any collaborative public information sites such as Wikipedia.

2.4 This policy applies to all use of the internet, and includes electronic communication devices such as e-mail, mobile phones, games consoles, social networking sites, and any other systems that use the internet for connection and providing of information. This would include use of both College owned and non-college owned devices as outlined in the Bring Your Own Device Policy.

2.5 This policy applies to all employees of the College. In addition, all individuals who work on the College premises or off-site on behalf of the College including agency, contract workers and volunteers are expected to read and abide by this policy.

3. Objectives

- To ensure college stakeholders follow the correct laws and regulations in the interest of both the law, and the business.
- To ensure college stakeholders utilise social media to the benefit of the business.
- To ensure stakeholders recognise and acknowledge their responsibility when using social media.
- To ensure safeguards on College IT-based systems are strong and reliable.
- To ensure user behaviour is safe and appropriate.
- To ensure that the storage and use of images and personal information on College IT- based systems is secure and meets all legal requirements.
- To educate stakeholders in e-safety.
- To ensure any incidents which threaten e-safety are managed effectively.

4. Intended Outcomes

4.1 Security

- College networks are safe and secure, with appropriate and up-to-date security measures and software in place.
- Digital communications, including email and internet postings, over the College network, are effectively monitored.
- Malicious activity is both prevented and recorded.
- Stakeholders are well enough informed to protect themselves and the business online and on social media.

4.2 Risk assessment

- When making use of new technologies, new social media sites, and online platforms, risk assessments are carried out.

4.3 Behaviour

- All users of technology adhere to the standards of behaviour set out in the Acceptable Use Policy.

- All users of IT adhere to College guidance when using email, mobile phones, social networking sites, games consoles, chat rooms, video conferencing and web cameras etc.
- Any abuse of IT systems and any issues of bullying or harassment (cyber bullying) are robustly dealt with, in line with staff disciplinary procedures.
- Any conduct considered illegal is reported to the police.

4.4 Use of Images and Video

- All stakeholders must ensure there is no breach of copyright or other rights of another person when using images and video online.
- Stakeholders are aware of the risks in downloading, posting, and sharing images, and particularly in the risks involved in posting personal images onto social networking sites, for example.
- College staff should provide information to learners on the appropriate use of images, and on how to keep their personal information safe.
- Staff must ensure advice and approval is gained from a senior manager in specified circumstances or if there is any doubt about the publication of any materials.
- Published photographs must not include names of individuals.

4.5 Personal Information

- Processing of personal information is done in compliance with the Data Protection Act 1998 and GDPR.
- Personal information is kept safe and secure and is not passed on to anyone else without the express permission of the individual.
- No personal information is posted to the College website/intranets without the permission of a senior manager.
- Staff always keep learner's personal information safe and secure.
- When using an online platform, all personal information is to be password protected.
- No personal information of individuals is taken offsite unless the member of staff has the permission of their manager.
- Every user of IT facility logs off on completion of any activity, or ensures rooms are locked if unsupervised, where they are physically absent from a device.
- Mobile devices that contain personal data (laptop, USB) are to be encrypted and password protected.
- Personal data no longer required, is to be securely deleted.

4.6 Education and Training

4.6.1 Staff – remote learning

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

4.6.2 Staff – Training

- Staff are supported through CPD to develop the skills to be able to identify risks independently and manage them effectively.
- Staff should provide inductions to learners and the programme of tutorials should include sessions on e-safety.
- Staff should guide learners in e-safety across the curriculum and opportunities are taken to reinforce e-safety messages.
- Staff should make learners aware of what to do and who to talk to if they have concerns about inappropriate content, either where that material is directed to them, or where it is discovered otherwise.
- Staff should encourage learners to question the validity and reliability of materials researched, viewed or downloaded. They should also be encouraged to respect the copyright of other parties and to cite references properly.
- Staff should complete e-Safety training as part of their CPD.
- Any new or temporary users receive training on the college IT system and they are also asked to sign the (staff) AUP

4.7 Incidents and Response

A clear and effective incident reporting procedure is maintained and communicated to learners and staff.

Reports of e-Safety incidents are acted upon immediately to prevent, as far as reasonably possible, any harm or further harm occurring.

4.7.1 Staff are expected to be ready to receive a report of an online safety incident and take the appropriate immediate action to prevent any harm and record enough details to report the matter to the Safeguarding Team following the College's Safeguarding Procedures.

4.7.2 Observations and concerns from staff members with regards to online safety incidents (i.e. a learner accessing material which may pose potential harm) should be reported to the Safeguarding Team following the College's Safeguarding procedures.

4.7.3 Reports via the College's IT monitoring and filter systems or breaches of the Computer Network, Internet and Intranet Acceptable Use Policy are likely to come to the attention of the IT Support Unit in the first instance. IT Support will then refer the matter to the Head of Student Services and/or the Safeguarding Team as appropriate.

4.7.4 Concerns regarding online safety incidents involving members of staff should be reported to the Principal, or Director of HR.

4.7.5 Action following the report of an incident might include; further investigation, support for the learner and affected learners, disciplinary action, sanctions, referrals to external agencies (e.g. social services, the police etc.), review of internal procedures and safeguards.

5. Legislation

5.1 The College will adhere to its obligations under the legislation relevant to the use and monitoring of electronic communications, which are predominantly:

- Regulation of Investigatory Powers Act 2000
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Communications Act 2003
- Data Protection Act 1998
- Human Rights Act 1998
- Defamation Act 1996
- Equality Act 2010
- General Data Protection Regulations 2016/679 *"GDPR"*

6. Data Protection and Monitoring

6.1 Computers and devices that are the property of the College are provided to assist in the performance of work duties. To ensure appropriate use of the internet, the College's firewall and web filter appliances are able to monitor all websites visited and connections made by employees. Therefore, users should have no expectation of privacy when it comes to the sites they access from College computers and devices.

6.2 The College may exercise its rights to intercept internet or email access under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 for the following business reasons:

- To establish the existence of facts relevant to the College's business.
- To ascertain compliance with regulatory practices or procedures relevant to the College.
- To ensure that employees using the system are achieving the standards required.
- To prevent or detect crime.
- To investigate or detect the unauthorised use or abuse of the telecommunications systems, including the use of social media sites.
- To ensure effective operation of systems, e.g. to detect computer viruses and to maintain an adequate level of security.

6.3 To be able to exercise its rights, the College must make all reasonable efforts to inform every person who may use the internet systems that monitoring may take place. The communication of this policy and the Acceptable Use Policy to all employees meets this requirement.

7. Privacy Settings and Personal Information

7.1 Default privacy settings for some social media websites allow some information to be shared beyond an individual's contacts. In such situations, the user of the site is personally responsible for adjusting the privacy settings for the account. Therefore, it is strongly encouraged to review their access and privacy settings for any social media sites to control, restrict and guard against who can access the information on those sites.

7.2 Even if privacy and security settings are utilised, staff should be aware that anything posted on social media sites may be made public by onward transmission or a change in a particular platform's privacy or sharing policy.

7.3 Social media offers the ability to share personal information rapidly and easily. Employees should be aware of the importance of setting and protecting secure passwords and restricting personal information to reduce the risks of abuses such as identity theft.

7.4 Any use of the college's name (including but not limited to: 'Oaklands College' on personal social media accounts and profiles is at the sole discretion of the user.

7.4.1 Any social media accounts that refer to the college's name as an employer or otherwise will be subject to periodic inspection, and the owners of such accounts may be liable to disciplinary action in the event of any inappropriate content found.

7.4.2 To avoid any confusion between the opinions of the business and the individual, use of the college's name in any social media profile must be accompanied by the statement
"Opinions are my own and do not reflect those of my employer."
Or similar.

8. Social use of email

Oaklands College accepts that staff and students may use their email accounts for personal or social use, this is permitted but you must follow the following guidelines.

Do · Keep usage of your staff email for personal or social use to an absolute minimum. · Keep email to outside parties polite and do not send offensive materials using a College email address. · Keep emails of a personal nature in a folder called "Personal", that way if there is a need to look in your mailbox any private emails can be kept private.

Do Not · Do not send emails that do not comply with the College's "Electronic Mail Messaging and Electronic Communication Policy." · Send large numbers of emails for social use, you should be aware that an investigation may be required if it is suspected you are sending large numbers

8.1 Use of Social Media at Work

8.1.1 Personal use of social media whilst at work

8.1.2 The College accepts that employees may wish to use social media channels as a way of communicating personally with the public and friends. Employees are permitted to make reasonable and appropriate personal use of social media websites from the College's IT network during official rest breaks and/or times when they are not on duty (i.e. before and after work) however its use at work must be restricted to the terms of this policy.

8.1.3 Employees may wish to use their own personal devices, such as laptops, hand-held devices and smart phones, to access social media websites while at work. Employees should be aware that the terms of this policy extend to this type of personal use.

8.1.4 The College IT Systems are first and foremost business tools, and as such personal usage of the systems is a privilege and not a right.

8.1.5 Personal use of social media should not interfere with employees' work duties and responsibilities. Excessive personal use or a failure to adhere to this policy may result in disciplinary proceedings.

8.2 Work-related use of social media

8.2.1 Employees are permitted to make reasonable and appropriate use of social media websites during working time where this is part of their normal duties, or as a particular project. This use must be authorised by their line manager.

8.2.2 The College operates a number of social media accounts on various platforms. Social media is an important part of how the College communicates and interacts with its employees, students and other stakeholders. Employees with responsibility for contributing to the College's social media activities must always be mindful that they are representing the College.

9. Rules for Use of Social Media in a Work-Related Capacity

9.1 Employees whose role includes the use of social media in an official capacity for promoting the College, teaching and research should adhere to the following rules:

- Official postings to official college sites are to be made only by those staff specifically authorised to do so by the Principal, or Director of Marketing and Communications.
- Members of staff may contribute to or interact with any posting on an official account subject to the terms of this policy (eg 're-tweeting' a message or 'liking' or adding a comment to a posting.
- Where any negative posting about the College, its employees or work is made on a social networking site (whether a College account or otherwise), staff should not reply or react to the posting in any capacity. If any member of staff notices such a posting they should report it to the Director of Marketing and Communication. The exception to this is for the College's official accounts where the staff member specifically responsible for that account may respond using their professional judgement and taking the advice of their line manager where appropriate.

- If a staff member or a department wishes to create a social media account to use for College business, they must get the approval of a member of the College Leadership Team and the Director of Marketing and Communication.
- The Director of Marketing and Communication will keep a register of College accounts and monitor their use, ensuring that it is appropriate to the College's communication strategies, reputation and standing.
- Staff members must not create an account on any social media platform under a name similar to that of the College, or that could in any way be associated with or confused with an official College account. This would include, for example, setting up an account purporting to be that of another member of staff.

10. Expected Standards of Conduct on Social Media Websites

10.1 The line between public and private, professional and personal is blurred when using social media. If an employee in any way makes themselves identifiable as a member of staff at the College, this has the potential to create perceptions about the College to a range of external audiences and also among colleagues and students.

10.2 These guidelines apply when using the College's own social media accounts, personal accounts or any third party accounts.

10.3 Appropriate conduct

10.3.1 When communicating via any social media platform, either in a professional or personal capacity, within or outside the workplace, employees **must**:

- Conduct themselves in accordance with other policies, procedures, and the College Code of Conduct.
- Be professional, courteous, and respectful as would be expected in any other situation.
- Think carefully about the impact of any posting or contribution made on social media sites.
- Be transparent and honest. The College will not tolerate employees making false representations. If employees express personal views, it should be made clear that the views do not represent or reflect the views of the College.
- Remove or request the removal of any inappropriate postings, comments, images or videos about them.

10.4 Inappropriate conduct

10.4.1 When communicating through social media either in a professional or personal capacity, within or outside the workplace, employees **must not** conduct themselves inappropriately. The following are examples of inappropriate conduct:

- Engaging in activities that have the potential to bring the College into disrepute.
- Breach of confidentiality by disclosing privileged, sensitive and/or confidential information.
- Making comments that could be interpreted as bullying, harassing or discriminatory.
- Commenting on any work-related matters.
- Doing anything that may conflict with the interests of the College.
- Posting remarks which may reasonably be considered to cause offence.

- Posting or uploading inappropriate comments, images, photographs or video clips about colleagues or ex-colleagues, students or ex-students, parents, clients, or any other stakeholder of the College.
- Publishing defamatory opinions or information and/or false material about the College, other employees, or students.
- Creating an account or posting material purporting to come from another member of staff, student, or any other individual. This includes creating an account that could reasonably be confused with the College.
- Posting a comment or opinion that purports to represent the views of the College, unless approved by the member of staff responsible for the College's social media accounts.
- Posting material which may contravene the College's equality and diversity policy.
- Use of offensive, derogatory, or intimidating language which may damage working relationships.
- Pursuing personal relationships with students, or ex-students under the age of 18, or parents of current students.
- Participating in any activity which may compromise your position at the College.
- Behaviour that would not be acceptable in any other situation.
- Knowingly accessing or downloading material which is illegal.
- Posting any material that breaches copyright legislation.
- Using a College email account to create a personal social media account.
- Using social media websites in any way which is deemed to be unlawful.

10.4.2 The above examples are not exhaustive or exclusive.

10.4.3 Employees will be held personally liable for any material published on social media websites that compromise themselves, their colleagues, and/or the College.

11. Relationships on Social Media Websites

11.1 The College encourages the positive use of social media as part of the educational process. Social media are used by many people, particularly students to communicate with their peers and the public and by the College itself, on official, rather than personal pages of websites such as Facebook. However, employees must not form personal relationships with any students, or ex-students under the age of 18, or parents of current students and must ensure that professional boundaries are always maintained. Entering such relationships through social media websites may lead to abuse of an employee's position of trust, and breach the standards of professional behaviour and conduct expected at the College.

11.2 Any safeguarding concerns of acts of a criminal nature will be referred to the College's Designated Safeguarding person and may subsequently be referred to the police, Local Safeguarding Children Board (LSCB) and/or the Independent Safeguarding Authority (ISA).

12. Responsibilities

12.1 All employees are responsible for complying with the requirements of this policy and for reporting any breaches of the policy to their line manager.

12.2 If employees have concerns about information or conduct on social media sites that are inappropriate, offensive, demeaning or could be perceived as bullying, this should be reported to their line manager immediately.