Social media and E-safety policy – Students

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 student life 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 students 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 students of the College when using social media either personally or for learning purposes, to manage 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
- Acceptable Use Policy
- Student behaviour 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 students 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 students follow the correct laws and regulations in the interest of both the law, and the college
- To ensure students utilise social media to the benefit of their learning.
- To ensure student 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 students 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.
- While using college devices or the college Wi-Fi, network and internet, you will be protected through the college firewall, web and spam filters which will block any inappropriate online material.
  If you are using a personal device or only connected to your mobile network then the responsibility is the owner of that device
- Digital communications, including email and internet postings, over the College network, are effectively monitored.
- Malicious activity is both prevented and recorded.
- Students should be well enough informed to protect themselves online and on social media.

4.2 Behaviour

- All users of technology adhere to the standards of behaviour set out in the Acceptable Use Policy and student behaviour 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 inappropriate behaviour(cyber bullying) are robustly dealt with, in line with student disciplinary procedures.
- Any conduct considered illegal is reported to the police.

4.3 Use of Images and Video

- All students must ensure there is no breach of copyright or other rights of another person when using images and video online.
- Students must be 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.
- The College should provide information to students on the appropriate use of images, and on how to keep their personal information safe.
- Students must ensure advice and approval is gained from a senior college manager in specified circumstances or if there is any doubt about the publication of any materials.
- Published photographs must not include names of individuals.

4.4 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 student, parent or guardian.
- Student personal information is kept safe and secure, through network security and back-ups
- When using an online platform, all personal information is to be password protected.
- No personal information of individuals is taken offsite unless has permission has been given
- 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.

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 teaching and learning. 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 Acceptable Use Policy to all students meets this requirement.

7. Online Safety

7.1 Cyberbullying can include:

- sending threatening or abusive text messages
- creating and sharing embarrassing images or videos
- trolling – the sending of menacing or upsetting messages on social networks, chat rooms or online games
- excluding children from online games, activities or friendship groups
- shaming someone online
- setting up hate sites or groups about a particular child
- encouraging young people to self-harm
- voting for or against someone in an abusive poll

- creating fake accounts, hijacking or stealing online identities to embarrass a young person or cause trouble using their name
- sending explicit messages, also known as sexting
- pressuring children into sending sexual images or engaging in sexual conversations.

While using college devices or the college Wi-Fi, network and internet you will be protected through the college web and spam filters which will block any inappropriate online material

If you are using a personal device or only connected to your mobile network

Then please follow the recommendations and guidelines below to ensure you are kept safe online

Report bullying on social media and online gaming guidance for students, parent, and carers

As well as supporting your child emotionally, there are practical steps you can take if the bullying has taken place on an online platform, such as a social media app or online gaming chat room.

- Don't stop them from using the internet or their mobile phone. It probably won't help keep them safe, it may feel like they're being punished and could stop them from telling you what's happening.
- Make sure your child knows how to block anyone who posts hateful or abusive things about them on each app or online service they use. You can usually find details of how to do this in the help or online safety area, under Settings.
- Report anyone who is bullying your child to the platform that's carried the offending comments, audio, image or video. Follow these links to contact some of the most popular social media platforms and learn more about blocking and reporting:
  Instagram> Snapchat>
  WhatsApp> Facebook>
  Skype>
- You can find details of more apps and games children and young people use, and how to contact them, on our Net Aware site.
- Thinkuknow has advice on online safety for young people that's suitable for different age groups. The website shows children how to contact social media sites if they believe someone has posted something upsetting about them.
- Block'em is a free app for Android users that blocks unwanted calls and text messages from specified numbers. Its website also provides advice for iOS users.
- Worried about how to support a young person who has had a sexual image or video of themselves shared online? If they're under 18, they can use Childline and the Internet Watch Foundation's discreet Report Remove tool to see if it can be taken down. Young people can get support from Childline throughout the process.

Report bullying videos shared online

- Get in contact with the site the video's been shared on as soon as possible. Social networks are more likely to take the video down if the child involved in the video or their parents make the report. Depending on their terms and conditions, they may be able to remove it from the site. You can visit Net Aware, in partnership with O2 - your guide to apps, games and social media sites to support you.