OISE Oxford E-Safety & Social Media Policy 2019

This policy relates to all members of the OISE Oxford community (including learners, staff, visitors and contractors) who have access to, and are users of ICT systems and resources both in and out of learning venues where actions relate to school set activities or use of school online systems.

Context:

To prepare learners for the needs of today and their future working lives where the curriculum and their personal goals require them to learn how to locate, retrieve and exchange information using a variety of technologies. Computer skills are vital to access employment and life-long learning as ICT is now seen as an essential skill for life. However, technologies present risks to vulnerable groups as well as benefits. Internet use for work, home, social and leisure activities is expanding across all sectors of society. This brings our staff and learners into contact with a wide variety influences some of which may be unsuitable.

These new technologies are enhancing communication and the sharing of information, which inevitably challenge the definitions and boundaries of the school environment. Current and emerging technologies in school and more importantly, in many cases outside the school by learners include:

Internet websites
Instant messaging
Social networking sites
Emails
Blogs
Podcasting
Video broadcasting sites
Chat rooms
Gaming and gambling sites
Music download sites
Mobile phones with camera and video functionality
Digital cameras
Smart phones, tablets and computers with e-mail and web applications

All of these have potential to help raise standards of teaching and learning, but may equally present challenges to both learners and tutors in terms of keeping themselves safe.

These challenges include:

Exposure to inappropriate material
Cyber-bullying via websites, social media, mobile phones or other technologies
Identity theft or invasion of privacy
Downloading copyrighted materials

Exposure to inappropriate advertising, online gambling and financial scams
Safeguarding issues such as grooming (children or vulnerable adults)
Other illegal activities

At OISE Oxford we seek to maximise the educational benefit that can be obtained by exploiting the use of ICT, whilst at the same time minimising any associated risks. By making clear to learners, staff, contractors etc. what the school expectations are regarding the use of ICT, we aim to protect our learners and staff from harm, as far as reasonably practicable. The precise nature of the risks faced by users will change over time as technologies, fads and fashions change but there are general principles of behaviour and the code of conduct that apply to all situations e.g.: all users need to know what to do if they come across inappropriate material, and that staff members should not give out their personal information to learners such as their personal telephone numbers, email address or allow access to their personal social networking site accounts etc. We must also communicate to our students on courses that they should not give out their personal information such as telephone numbers; addresses etc. to strangers or publish this information on social networking sites.

A balance needs to be struck between educating staff and learners to take a reasonable approach towards the use of regulation and technical solutions. We must recognise that there are no totally effective solutions to moderate and control the internet, so this policy incorporates both approaches.

Roles and Responsibilities

Staff

All teaching and non-teaching staff (including suppliers and contractors) are responsible for supporting the safe behaviour throughout the school and following e-safety procedures. All school staff should be familiar with the e-safety and social media policy as well as their relevance to the code of conduct and safeguarding policies, which are available on the school website. A copy of this policy will also be included in the staff handbook.

. All staff should participate in any e-safety training and awareness raising sessions
. Staff should act in accordance with the e-safety and social media policy
. Staff should report any suspicion of misuse to the designated persons or line manager
. Staff should refrain from making negative comments about learners or OISE Oxford on any blogs or social networking sites. Negative comments such as these could be considered as gross misconduct as it potentially affects the reputation of the school and/or lowers morale.
. Staff should help educate learners in keeping safe, especially with vulnerable groups. Whilst regulation and technical solutions (such as filtering systems) are important, they must be balanced with educating learners to take a responsible approach. The education of learners in e-safety is an essential part of using technology in classes.
. Staff should act as a good role model in their own use of ICT.
. Where Internet use is pre-planned in sessions or enrichment activities, learners

should be directed to sites which are appropriate for their use and procedures should be followed for reporting any unsuitable material that is found on Internet searches. Where practicable staff should pre-check sites and any possible searches.
. Where learners are able to freely search the Internet such as in our common rooms staff should be vigilant in monitoring the content of websites in case there is any unsuitable material.
. Staff should be aware of the potential for cyber-bullying in their sessions where malicious messages e.g. through the use of forums and social networking sites, or via internal class emails or text messages on mobile phones etc, which can cause hurt or distress.
. Learners should be taught to be critically aware of the materials/content they can access online and be guided to validate the accuracy of information.
. Learners are educated about the need to acknowledge the sources of any information used and to respect copyright when using material accessed on the Internet.
. Staff are required to use the BCC address label when sending emails to groups of students to prevent circulation of emails.

Learners

The provision of ICT resources and facilities are a privilege, not a right. Learners are encouraged to access various technologies in lessons and in the completion of assignments and independent research, and are therefore expected to follow the school's e-safety and social media policy. They should fully participate in e-safety activities and report any suspected misuse to a member of staff. Learners are required to follow the guidelines of our e-safety policy which are summarized in the code of conduct.

Learners are expected to:

. behave in a safe and responsible manner
. treat equipment with respect
. use USB/Flash memory key(s) only for educational purposes
. be polite and not use e-mail, social media or blogs etc to make negative comments, bully or insult others
. use the resources only for educational purposes

Learners are expected not to:

. waste resources including Internet and printers
. eat or drink in the ICT suites
. have any inappropriate files (e.g. copyrighted or indecent material)
. attempt to circumvent or "hack" any systems.
. use inappropriate or unacceptable language
. reveal their personal details or passwords
. visit websites that are offensive in any way
. use chat rooms or newsgroups
. do anything that could damage the reputation of the school
. download anything inappropriate or install any programs

School Management

The school management team takes e-safety very seriously and will ensure that policies and procedures are in line with best practice and the safeguarding agenda. In particular they will ensure that all staff receive suitable training and development to carry out their e-safety roles and sufficient resources are allocated to the task. Senior managers will follow the correct procedure in the event of a serious e-safety allegation being made against a member of staff and ensure that there is a robust system in place for monitoring e-safety. This includes making sure that the academic network infrastructure is safe and secure and that policies and procedures approved within this policy are implemented. Regular review of the issues will take place at the safeguarding working group meetings with feedback sessions scheduled to the senior management team meetings.

Responding to issues

It is important that any incidents are dealt with as soon as possible in a proportionate manner and that members of the school community are aware those incidents have been dealt with. Any concerns around the misuse of ICT must follow the referral process within the safeguarding policy and procedure where there is a potential threat to another learner, vulnerable person or member of staff. Any suspected misuse must be reported to a member of staff and then an appropriate course of actions will be agreed.

Where it is suspected that any misuse might have taken place and depending on the nature of misuse, the disciplinary procedure will be invoked. Where an allegation has been made against a student an investigation will take place by the Principal or the Designated Safeguarding Lead. The outcome of the investigation will decide what the appropriate course of action will be and depending on the nature of the misuse, the student could be suspended from classes till the investigation is complete. The student code of conduct procedure will be invoked should the allegation be found to be true and the sanction will depend on the seriousness of the misuse and whether it was accidental or deliberate, a first time offence, thoughtless or malicious e.g. intended to cause harm to others. Sanctions could involve the student having ICT access removed for a period of time or in very serious cases, exclusion. Where there is a potential legal issue the Principal will decide on the need for involvement of outside agencies including the police, together with the designated persons and other members of the senior management team in line with our safeguarding and other policies.

Social Media Policy

About this policy

This policy is in place to minimise the risks to our business through use of social media. It deals with the use of all forms of social media, including Facebook, LinkedIn, Twitter, Google+, Wikipedia, Whisper, Instagram, Vine, Tumblr and all other social media platforms, internet postings and blogs. It applies to use of social media for business purposes as well as personal use that may affect our business in any way. This policy does not form part of any employee's contract of employment and we may amend it at any time.

Personnel responsible for implementing the policy

Digital marketing executives from each respective brand within Instill Education have specific responsibility for managing their entire brand presence online and should always be consulted with any proposals concerning company social media channels, blogs and websites. In particular, no new social media accounts may be created, or use of brand names and logos online, without prior consultation and approval from digital marketing managers relevant to the brand in question. Managers have a specific responsibility for operating within the boundaries of this policy, ensuring that all staff understand the standards of behaviour expected of them and taking action when behaviour falls below its requirements. Managers will be given training in order to do this.

All staff are responsible for the success of this policy and should ensure that they take the time to read and understand it. Any misuse of social media should be reported to a manager. Questions regarding the content or application of this policy should be directed to your line manager.

Compliance with related policies and agreements

Social media should never be used in a way that breaches any of our other policies. If an internet post would breach any of our policies in another forum, it will also breach them in an online forum. For example, you are prohibited from using social media to:

.breach our Information and Communications Systems Policy
.breach our obligations with respect to the rules of relevant regulatory bodies
.breach any obligations contained in those policies relating to confidentiality
.breach our Disciplinary Policy or procedures
.breach our Anti-harassment and Bullying Policy
.unlawfully discriminate against other staff, students or third parties
.breach our Data Protection Policy (for example, never disclose personal information about a colleague or student online); or
.breach any other laws or regulatory requirements

Staff who breach any of the above policies will be subject to disciplinary action up to and including termination of employment.

Personal use of social media

Occasional personal use of social media during working hours is permitted so long as it does not involve unprofessional or inappropriate content, does not interfere with your employment responsibilities or productivity and complies with this policy.

Prohibited use

You must avoid making any social media communications that could damage our business interests or reputation, even indirectly.

You must not use social media to defame or disparage us, our staff, our students or any third party; to harass, bully or unlawfully discriminate against staff, our students or third parties; to make false or misleading statements; or to impersonate colleagues, students or third parties.

You must not express opinions on our behalf via social media, unless expressly authorised to do so by your manager. You may be required to undergo training in order to obtain such authorisation.

You must not post comments about sensitive business-related topics, such as our performance, or do anything to jeopardise our trade secrets, confidential information and intellectual property. You must not include our logos or other trademarks in any social media posting or in your profile on any social media.

Any misuse of social media should be reported to your line manager.

Business use of social media

Digital marketing executives are responsible for online external communications and engaging with their respective communities, and operate freely under guidelines agreed with their managers, who are ultimately responsible for what is published. If it is not part of your normal duties to speak on behalf of the organisation in a social media environment, you must seek approval for such communication from digital marketing representatives for your brand and your manager, who may require you to undergo training before you do so and impose certain requirements and restrictions with regard to your activities.

Likewise, if you are contacted for comments about the organisation for publication anywhere, including in any social media outlet, direct the enquiry to a digital marketing representative.

The use of social media for business purposes is subject to the remainder of this policy.

Guidelines for responsible use of personal social media

In any personal social media accounts you may use that are not affiliated with the company, it should be clear that you are speaking on your own behalf. Pay particular attention to any social media posts that are fully public and that bear your name, which could be connected to your affiliation with the company, and be aware that you are personally responsible for such communications published on the internet for anyone to see.

If you disclose your affiliation with us on your profile or in any social media postings, it must be clear that your views do not represent those of your employer (unless you are authorised to speak on our behalf as set out above). You should also ensure that any publicly accessible profile and any publicly accessible content you post are consistent with the professional image you present to clients, colleagues and students.

If you are uncertain or concerned about the appropriateness of any statement or posting, refrain from posting it until you have discussed it with your manager.

If you see social media content that disparages or reflects poorly on us, you should contact the digital marketing representatives for your brand and your manager.

Monitoring

We reserve the right to monitor, intercept and review, without further notice, staff activities using our IT resources and communications systems, including but not limited to social media postings and activities, to ensure that our rules are being complied with and for legitimate business purposes and you consent to such monitoring by your use of such resources and systems. For further information, please refer to our Information and Communications Systems Policy.

Recruitment

We may use internet searches to perform due diligence on candidates in the course of recruitment. Where we do this, we will act in accordance with our data protection and equal opportunities obligations.

Breach of this policy

Breach of this policy may result in disciplinary action up to and including dismissal. Any member of staff suspected of committing a breach of this policy will be required to co-operate with our investigation, which may involve handing over relevant login details.

You may be required to remove any social media content that we consider to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

Reviewed January 2019

To be reviewed January 2020