E-Safety Polcy

1.6 – August 2022

Contents

Creation and Revision History

To be reviewed annually by Head of Student Services. Next review due September 2022.

Version	Owner	Purpose/Change	Date
1.0	Simon Duckworth, Head of Student services	Creation of new policy to replace Student Social Media Policy	September 2017
1.1	Simon Duckworth, Head of Student Services	Annual review – no changes	September 2018
1.2	Simon Duckworth, Head of Student Services	Annual review – no changes	September 2019
1.3	Simon Duckworth, Head of Student Services	Annual review – amendment to hyperlink	September 2020
1.4	Simon Duckworth, Head of Student Services	Annual review – no changes	September 2021
1.5	Simon Duckworth, Head of Student Services	Addition of cybercrime - section 15	November 2021
1.6	Simon Duckworth, Head of Student Services	Roll to role	August 2022

1 Introduction

1.1 INTO UEA recognises the benefits and opportunities which new technologies offer to all our students and staff. We encourage the use of technology not only to enhance students' learning experience but also to promote skills and achievement. However, the accessible and global nature of the internet and associated technologies means that we are also aware of the potential risks faced and challenges involved.

1.2 Our approach is to implement safeguards within the centre which will support staff and students to manage any potential risks and to deal with these risks independently. We believe that this can be achieved through a combination of security measures, training, guidance and implementation of our associated policies.

1.3 The technologies encompassed within this policy include all computer based technologies, online communication technologies, digital technologies both fixed and mobile.

1.4 In addition, we will do all that we can to ensure that all of our students and staff stay e-safe within our duty of care.

1.5 This E-Safety Policy should be read in conjunction with other relevant policies, in particular the University Conditions of Computer Use, the Social Media Guidelines as shown at Appendix A, the Staff Handbook and the Safeguarding Policy.

2 INTO UEA E-Safety Policy

2.1 The aim of this policy is to develop a co-ordinated approach to e-safety and to promote and safeguard the welfare of all staff and students in a digital world. This will be achieved without hindering students' e-learning experience, whilst ensuring that skills and knowledge are developed to maximise the use of technology in an appropriate manner.

3 Terminology

3.1 Terminology used throughout this document is as follows:

- Site = Facebook or similar.
- Account = login (e.g. personal and/or work – you log into your account, using your account login details).
- Profile (Profile Page) = a page that shows personalised information added to your account. E.g. my personal Facebook profile page is accessed using my personal account details.
- Portal = an internet portal is a website that acts as a starting point for browsing the web. Portals typically include search engines and large directories of websites. There are also many smaller portals, known as "niche portals" for specific interests.

4 Policy Scope

4.1 This policy applies to all students and staff (including agency staff and contractors) of the centre community and the use they make of the internet and electronic communication devices such as email, mobile phones, games consoles and social networking sites, whether using college systems or resources of their own. This policy also applies to behaviour towards other people in centre using private mobiles.

5 Roles and Responsibilities

5.1 There are clear guidelines and lines of responsibility for e-safety within the centre. The first point of contact should be the Head of Student Services or a member of the Safeguarding Team. All staff are responsible for ensuring the safety of students and should report any concerns immediately to their line managers.

5.2 As with the centre Safeguarding Policy – staff should take care not to guarantee any measure of confidentiality to any individual reporting any concerns regarding e-safety.

6 Security

6.1 INTO UEA and UEA will do all it can to ensure that the network is safe and secure. Every effort will be made to keep security software up to date and fit for purpose. Appropriate security measures will include the use of enhanced filtering and protection of firewalls, servers, routers, work stations to prevent malicious or accidental access of systems and information. Digital communications, including emails and internet postings over the network, will be monitored in accordance with the University Conditions of Computer Use.

6.2 Internet usage and monitoring is in place, use of accounts that are password protected enable detailed monitoring to take place, and users also have their own storage and email accounts that are also subject to monitoring.

7 Behaviour

7.1 Online communication and computer use can take many forms, whether via email, text, video conferencing or instant chat/messaging. The centre will ensure that all users of technologies adhere to the expected standard of behaviour as set out in the University Conditions of Computer Use.

- https://www.uea.ac.uk/about/university-information/university-governance/academic-calendar/section-3/general-regulations/conditions-of-computer-use

7.2 INTO UEA will not tolerate any abuse of ICT systems or associated technologies. Whether offline or online, communications by staff and students should be courteous and respectful at all times, please refer to the Staff Handbook. Any reported incident or bullying, harassment or other unacceptable behaviour will be treated seriously as set out in the Student Code of Conduct and Disciplinary Policy and/or the Staff Handbook.

7.3 Where conduct is found to be unacceptable, the centre will deal with this internally. Where conduct is considered illegal, the matter will be referred to the Police. Additionally, the centre may seek to involve other agencies where conduct is believed to be unacceptable or illegal.

8 Communications

8.1 There is a wealth of technologies now available to enhance communication with one another. It is noted that this policy will require continual updating in line with the evolving nature of e-technology and associated communication methods. Electronic communication included:

- Internet collaboration tools: social networking sites and blogs;
- Internet research: websites, search engines and web browsers;
- Mobile phones and personal digital assistants (PDAs);
- Internet communications: email and instant messaging;

- Webcams and video conferencing;
- Wireless games consoles.

9 Data Protection/Personal Information

9.1 Any processing of personal information must be carried out in accordance with the Data Protection Act 1998.

9.2 INTO UEA collects and stores the personal information of staff and students regularly e.g. names, dates of birth, email addresses, assessment materials and so on. The centre will keep that information safe and secure and will not pass any information onto anyone else without the express permission of the member of staff, student, parent or carer.

9.3 No personal information can be posted to the centre website without the permission of the person concerned, or their parent or carer.

9.4 Staff must keep students' personal information safe and secure at all times. When using an online platform, all personal information must be password protected and every user is required to log off on completion of any activity.

10 Use of Images and Videos

10.1 The use of images, photographs and videos is particularly popular to promote the outstanding work carried out in different curriculum areas, this practice should be encouraged where there is no breach of copyright or the rights of another person. This includes downloading images from the internet and images belonging to staff and students.

10.2 No images, photographs or videos can be copied, downloaded, shared or distributed online without permission from the person. Photographs taken during centre activities will be considered carefully and have the consent of the person involved before being published. Unauthorised use of images of the centre and/or staff and students will be seen as a breach of the policy, including images or photographs that have been altered.

11 Education and Training

11.1 With the current unlimited nature of internet access, it is impossible for the centre to eliminate all risks for staff and students. It is our view, therefore, that INTO UEA should support staff and students through training and education. This will provide all users with the necessary skills to be able to identify risks and deal with them independently and manage them effectively.

12 Staff (including agency staff and contractors)

12.1 Staff will be offered e-safety guidance through annual safeguarding training offered to all staff and including information and themes from this policy.

13 Students

13.1 Students will receive e-safety and social media guidance during their induction. Students' will also receive guidance on copyright and plagiarism embedded in their learning curriculum.

14 Incidents and Reporting

14.1 Where an e-safety matter is reported, the matter will be dealt with very seriously. The centre will act immediately to prevent, as far as is reasonably possible, any harm or further harm occurring. If a student wishes to report an incident, they can so to any member of staff. When a member of staff wishes to report an incident they must inform a member of the safeguarding team.

14.2 Following any reported incident a full investigation will be carried out and the centre will decide on the most appropriate course of action. Sanctions may be put in place, external agencies may be contacted or the matter resolved internally depending on the seriousness of the incident. Serious incidents will be dealt with by senior management, in consultation with appropriate

15 Cybercrime

15.1 We understand that cybercrime is criminal activity committed using computers and/or the internet. It is broadly categorised as either 'cyberenabled' (crimes that can happen off-line but are enabled at scale and at speed on-line) or 'cyber dependent' (crimes that can be committed only by using a computer). We are also aware that international students may be targeted and particlualry vulnerable to cybercrime.

15.2 INTO UEA works closely with local police and national cybercrime agencies where appropriate to respond to an incident in which a student has been a victim of cyber crime and also to promote safer online behaviour among our student body

16 Further Information

16.1 Useful links for further information:

- http://www.getsafeonline.org
- http://www.thinkuknow.co.uk/
- http://cybermentors.org.uk/
- http://digizen.org.uk/
- http://www.childnet-int.org/blogsafety/yp.html

Appendix A Social Media Guidelines

Introduction

Social media portals are powerful communication tools that have a significant impact on organisational and professional reputations. Because they blur the lines between personal voice and institutional voice the following guidelines are designed to help clarify how best to enhance and protect personal and professional reputations when participating in social media.

Social media portals are defined as media designed to be disseminated through social interactions, created using highly accessible and scalable publishing techniques. Examples include, but are not limited to, LinkedIn, Twitter, Facebook, YouTube and WeChat. Both in professional and institutional roles, employees need to follow the same behavioural standards online as they would in real life. The same laws, professional expectations, and guidelines for interacting with students, parents, the media etc. apply online as in the real world. Staff are liable for anything they post to social media sites.

Guidelines for all social media sites, including personal sites

Protect confidential and proprietary information: do not post confidential or proprietary information about the centre, its students or employees. The Data Protection Act is very specific with regard to the disclosure of personal information without the consent of the owner; any disclosure could result in criminal action against the individual and the centre and may result in disciplinary action.

When posting, be mindful of the copyright and intellectual property rights of others and of INTO UEA.

Do not use the INTO UEA logo on personal social media sites. Do not use the centre's name to promote a product, cause or political party or candidate.

In accordance with the University Conditions of Computer Use you may access personal social media portals only at specified times and locations.

All staff should ensure that personal social networking sites are set to private and that current students are never listed as approved contacts.

Obey the Terms of Service of any social media platform employed.

Best Practices

This section applies to your general use of social media portals in any capacity; it is intended as advice for personal use or as a standard for use associated with the centre.

Think twice: before posting, privacy does not exist in the world of social media. Consider what could happen if a post becomes widely known and how that may reflect both on the poster and the centre. Search engines can turn up posts years after they are created, and comments can be forwarded or copied. If you wouldn't say it at a conference or to a member of the media, consider whether you should post it online.

Strive for accuracy: get the facts straight before posting them on social media. Review content for grammatical and spelling errors.

Be respectful: understand that content contributed to a social media site could encourage comments or discussion of opposing ideas. Responses should be considered carefully in light of how they would reflect on the poster and/or the centre.

Remember your audience: be aware that a presence in the social media world is, or easily can be, made available to the public at large. This includes prospective students, current students, current employers, colleagues and peers. Consider this before publishing to ensure the post will not alienate, harm, or provoke any of these groups.

Acknowledge who you are: on personal sites identify your views as your own. If you identify yourself as a staff member or student of INTO UEA, it should be clear that the views expressed are not necessarily those of the centre.

Photographs: posted on social media sites can be appropriated by visitors and altered to convey a different meaning to the original.

Have a plan: staff should consider their messages, audiences, and goals, as well as a strategy for keeping information on social media sites up-to-date.

Link back to the centre: staff posting as part of work-related activity should do so on authorised INTO UEA social media accounts.

Protect the centre's reputation: posts on social media sties should protect the centre's reputation by remaining professional in tone and good taste. No individual staff members or students should construe their social media site as representing the centre.

Be aware of liability: you are legally liable for what you post on your own site and on the sites of others. Individual bloggers have been held liable for commentary deemed to be proprietary, copyrighted, defamatory, libellous or obscene.

Work related social media

It is recognised that using social media portals as a teaching and learning aid is beneficial; these guidelines are designed to avoid any pitfalls when they are used as part of your working role in the centre. Social media should not be seen as negative, there are many sites that can seriously enhance a learning environment and provide an excellent way of communicating with students.