ONLINE SAFETY POLICY

Introduction

1. The University of Suffolk recognises the benefits and opportunities which new technologies offer to teaching and learning. We provide internet access to all students and staff and encourage the use of technologies in order to enhance skills, promote achievement and enable lifelong learning. However, the accessibility and global nature of the internet and different technologies available mean that we are also aware of potential risks and challenges associated with such use. Our approach is to implement appropriate safeguards within the University while supporting staff and students to identify and manage risks independently and with confidence. We believe this can be achieved through a combination of security measures, training, guidance and implementation of our policies. In furtherance of our duty to safeguard students, we will do all that we can to make our students and staff stay e-safe and to satisfy our wider duty of care. This Online Safety Policy should be read alongside other relevant policies e.g. Acceptable Use Policy, Safeguarding Policy, Use of IT Facilities, Data Protection Policy, Dignity at Study, Student and Staff Disciplinary Procedures, Professional Use of Social Media, Social Media Toolkit and General Regulations.

Scope

2. The Policy applies to all students and staff of the University of Suffolk who have access to the IT systems, both on the premises and remotely. The Online Safety Policy applies to all use of the internet and forms of electronic communication such as email, online learning environment (MySuffolk and Brightspace), mobile phones, and social media sites. Any user of the University IT systems must adhere to policies and guidance as published on MySuffolk.

Roles and Responsibilities

3. All staff are responsible for ensuring the safety of students and should report any concerns immediately to their line manager. All teaching staff are required to familiarise themselves with the appropriate policy and guidance. Online Safety incidents are any instances where there is risk of harm, or actual harm, to an individual where digital technology has been used. For example, indecent images, online abuse, revenge pornography, radicalisation. When informed about an online safety incident, staff members must take particular care not to guarantee any measure of confidentiality towards either the individual reporting it, or to those involved.

4. All students must know what to do if they have online safety concerns and who to talk to. In most cases, this will be:

- Personal Tutor / Course Leader
- The Students' Union Advice Service

- Student Services (or relevant Welfare and Guidance Department at a Partner institution)
- Chaplaincy

Where appropriate, the Designated Safeguarding Officer may be asked to intervene with appropriate additional support from external agencies.

5. The ***Designated Safeguarding Officer*** will be expected to review and monitor the implementation of the Online Safety Policy and guidance and, through the Institution's corporate development programme, ensure that appropriate staff development and training takes place.

6. ***Students*** are responsible for using the IT systems and mobile devices in accordance with the University of Suffolk Use of IT Facilities Guidance, the Online Safety Policy, the Dignity at Study Policy and the Social Media Toolkit. Adherence to these policies is acknowledged at the point of enrolment. Students must act safely and responsibly at all times when using online technologies. They must follow reporting procedures where they are worried or concerned, or where they believe an online safety incident has taken place involving them or another member of the University community.

7. All ***Staff members*** are responsible for using IT systems and mobile devices in accordance with the University of Suffolk Use of IT Facilities Guidance, the Online Safety Policy, the Dignity at Study policy and the Social Media Toolkit. All digital communications with students must be professional at all times. All staff should apply relevant policies and understand the incident reporting procedures. Any incident that is reported to or discovered by a staff member must be reported to the Designated Safeguarding Officer or their deputies.

Security

8. The University of Suffolk will do all that it can to make sure the network is safe and secure. The University will ensure security software is kept up to date using standard auto updating carried out daily. Appropriate security measures will include the use of enhanced filtering and protection of firewalls, servers, routers, work stations etc. to prevent accidental or malicious access of systems and information. Digital communications, including email and internet postings, over the University network, will be monitored.

Risk Assessment

9. In making use of new technologies and external online platforms, all staff must consult with IT Services to first carry out a risk assessment for online safety. For examples of questions that might be included, refer to the JISC Legal Web 2.0 Tutor's Checklist.

Behaviour

10. The University of Suffolk will not tolerate any abuse of IT systems. Whether offline or online, communications by staff and students should be courteous and respectful at all times. Any reported incident of bullying, harassment or other unacceptable conduct will be treated seriously and in line with the Dignity at Study (Students) and Dignity and Respect at Work (Staff) policies, and relevant student and staff disciplinary procedures. Where conduct is found to be unacceptable, the University will deal with the matter internally. Where conduct is considered illegal, the University will report the matter to the police.

Use of Images, Video and Audio

11. The use of images photographs, video and audio is popular in teaching and learning and should be encouraged where there is no breach of copyright or other rights of another person (e.g. image rights or rights associated with personal data). This could include images, video or audio downloaded from the internet and those belonging to staff or students.

12. All students and staff should be aware of the risks when taking, downloading and posting images, video or audio online and making them available to others. There are particular risks where personal images, videos or audio clips of themselves or others are posted onto social networking sites, for example. The University will provide opportunities to students to gain information on the appropriate use of images, video and audio. Our aim is to reinforce good practice as well as offer further information for all users on how to keep their personal information safe.

13. No image, photograph, video or audio clip of an individual or group can be copied, downloaded, shared or distributed online without permission from the subject(s). Photographing, recording or videoing activities on University premises should be considered carefully; staff members are encouraged to notify participants of the likelihood of their photograph being taken or them featuring in videos or audio clips. Approved photographs, videos or audio clips should not include names of individuals without consent.

Personal Information

14. Personal information is information about a particular living person. The University of Suffolk collects and stores the personal information of students and staff regularly e.g. names, dates of birth, email addresses, physical addresses, assessed materials and so on. The University will keep that information safe and secure and will not pass it onto anyone else without the express permission of the data subject in line with data protection legislation.

15. No personal information can be posted to the University of Suffolk website without the permission of the data subject unless it is in line with our Data Protection Policy.

16. Staff must keep students' personal information safe and secure at all times. When using an online platform, all personal information must be password protected. Every user of IT facilities is required to log off on completion of any activity, or where they are physically absent from a device for any period.

17. Where the personal data is no longer required, it must be securely deleted in line with the Data Retention procedure.

Guidance and Training

18. With the current unlimited nature of internet access, it is impossible for the University to eliminate all risks for staff and students. It is our view, therefore, that the University should support staff and students to stay e-safe through the provision of guidance and training. This will provide individuals with skills to be able to identify risks independently and manage them effectively.

a) For students:

Online safety will form part of the Induction programme for new and returning students, supported by the guidance on MySuffolk. Follow up sessions will be available through Career and Employability workshops. During their studies, students will be encouraged to question the validity and reliability of materials researched, viewed or downloaded. They will also be encouraged to respect the copyright of other parties and to cite references properly.

b) For staff:

New staff will take part in online safety training as part of their induction. Existing staff will be encouraged to familiarise themselves with the policies and guidance, and to participate in the corporate development programme.

Incidents and Response

19. Where an online safety incident is reported to the University, the matter will be dealt with very seriously. The University will act to prevent, as far as reasonably possible, any harm or further harm occurring.

20. If a student wishes to report an incident, they can do so to their Personal Tutor or Course Leader.

21. Where a member of staff wishes to report an incident, they must contact their line manager as soon as possible.

22. Following any incident, the University will review what has happened and decide on the most appropriate and proportionate course of action. Sanctions may be put in place, external agencies may be involved or the matter may be resolved internally depending on the seriousness of the incident. Serious incidents will be dealt with by senior management, in consultation with appropriate external agencies.