## ONLINE BEHAVIOUR 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.

2.     This Online Behaviour Policy should be read alongside other relevant policies including Data Protection and Data Security Policy, Dignity at Study Policy, Fitness to Study Procedure, General Regulations (Students), IT Services Policies, Safeguarding Policy, Social Media Guide, Student Complaints Procedure, and Student Discipline Procedure.

3.     The policy is informed by the Universities UK guidance 'Tackling Online Harassment and Promoting Online Welfare' and the related case studies.

**Scope**

4.     The Policy applies to all students and staff of the University of Suffolk, including students studying with the University's academic partners. The Online Behaviour Policy applies to all use of the internet and forms of electronic communication such as email, online learning environment (including MySuffolk and Brightspace), mobile phones, messaging platforms and social media.

5.     Students studying with academic partners may also be subject to local or institution specific policies.

**Roles and Responsibilities**

**Staff**

6.      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. 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, technologically facilitated harassment, image based abuse (for example revenge pornography), radicalisation or hate speech. When informed about an incident, staff members must take particular care not to guarantee any measure of confidentiality towards either the individual reporting it, or to those involved.

7.      All digital communications by members of staff 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.

**Students**

8.      All students must know what to do if they have concerns related to online behaviour, how to report and who to talk to. In most cases, this will be:

- Personal Tutor / Course Leader
- The Students' Union Advice Centre
- Student Services (or relevant support service at a Partner institution)
- Multi-faith Chaplaincy

9.      Where appropriate, the Designated Safeguarding Officer (as defined in the Safeguarding Policy) may be asked to intervene, with appropriate additional support from external agencies.

10.      The Designated Safeguarding Officer will review and monitor the implementation of this policy and related guidance and, through the Institution's corporate development programme, ensure that appropriate staff development and training takes place.

11.      Students and staff 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 incident has taken place involving them or another member of the University community.

**Network Security**

12.    The University of Suffolk will take all necessary precautions to ensure 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.

**Behaviour**

13.    The University of Suffolk will not tolerate any abuse or harassment (including hate speech) online. 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 and Dignity and Respect at Work policies, and relevant student and staff disciplinary procedures. Where conduct is found to be unacceptable, the University will deal with the matter internally and in accordance with relevant procedures. Where conduct is considered illegal, the University will report the matter to the police and other relevant external agencies.

**Use of Images, Video and Audio**

14.    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 at induction and as part of the curriculum. Our aim is to reinforce good practice as well as offer further information for all users on how to keep their personal information safe.

15.    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) or copyright holder. 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. Photographs, videos or audio clips approved for use should not include names of individuals without additional, appropriate consent.

**Guidance and Training**

16.    With the 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 understand online risks 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 behaviour and safety guidance will form part of the Induction programme for new and returning students and will be updated through the curriculum, supported by the guidance on MySuffolk. During their studies, students will be encouraged to question the validity and reliability of materials researched, viewed or downloaded in order to enhance their ethical digital literacy skills. 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. Staff should be aware of relevant legislation, the university's duty of care to students, and know routes for reporting incidents and disclosures.

**Incidents and Response**

17.    If a student wishes to report an incident, they can do so to their Personal Tutor, Course Leader, Student Services or equivalent support service at a Partner institution, or to the Students' Union Advice Service. However, any member of staff at the University of Suffolk or a Partner institution should be responsive to any disclosure made.

18.    Where a member of staff wishes to report an incident, they must contact their line manager where possible or refer to the University's Whistleblowing policy. Staff employed by Partner institutions should refer to local policies for guidance in the first instance.

19.    Where an incident is reported to the University, the matter will be dealt with in line with the University's policies and procedures as detailed in Paragraph 2 above. The University will act to prevent, as far as reasonably possible, any harm or further harm occurring. 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.