

Online Safety Policy

Date: 10 June 2026

Last amended by: Tim Johnson

1 Introduction & Purpose

- 1.1 ThinkSpace Education (TSE) is committed to promoting the welfare and safety of our students when using digital and online technologies. TSE recognises the importance of the contribution it can make to protecting and supporting students in their use of these technologies.
- 1.2 This policy is designed to incorporate all aspects of safeguarding that may be affected by digital technology, as well as TSE's use of technology.

2 Scope

- 2.1 This policy applies to all TSE staff and students.
- 2.2 This policy applies to any individual who is given access to TSE's digitally connected systems.
- 2.3 The Online Safety policy covers the use of:
 - (a) The TSE VLE
 - (b) TSE related external Internet, including but not exclusively, extranet, e-learning platforms, blogs, social media websites and any other online platform used for TSE purposes
 - (c) External access to internal TSE networking and servers
 - (d) TSE equipment off-site, for example staff laptops
 - (e) Student and staff personal IT equipment when used in TSE premises and which makes use of TSE networking, file-serving or other TSE systems
 - (f) TSE-provided @thinkspace.ac.uk email accounts, which are TSE accounts subject to this policy
- 2.4 Students accessing Arts University Bournemouth (AUB) systems are also subject to AUB's Acceptable Use Policy when using those systems.

3 Policy Statement

- 3.1 The definition of an online incident is:
- 3.2 "Any incident that occurs and involves any person (student or staff) where the use of technology (equipment and/or networks) enables or facilitates inappropriate behaviour and harm and/or distress is caused to another person or the reputation of TSE. This may include the use of social media, forums, blogs, open and closed groups, digital images, messages or any other means".
- 3.3 The most likely areas of risk to students are:
 - (a) Exposure to illegal, inappropriate or harmful material
 - (b) Subject to harmful online interactions with other users
 - (c) The individual's personal online risky behaviour that then leads to harm
- 3.4 TSE has a responsibility for ensuring that the resources are available to promote the safe use of technology and to promote understanding and awareness of the risks attached to the use of digital technology.

- 3.5 We seek to promote the use of technology and connectivity to ensure that the students are equipped with the necessary skills and knowledge to perform to the best of their ability.
- 3.6 Staff and students must be able to use digital technology appropriately and safely and understand the risks related to their activity. Students will be able to access online safety education.
- 3.7 TSE actively encourages a proactive approach to new and emerging technologies and threats to mitigate the risk of harm to students, staff and TSE's reputation. We seek to promote a 'cyber aware' culture that ensures all staff and students continue to develop their knowledge and understanding of safe and appropriate online behaviours.

4 Standards and Expectations

4.1 Systems

- 4.1.1 TSE web resources and IT systems are configured to ensure the teaching and learning requirements of TSE are met whilst ensuring online safety is maintained.
- 4.1.2 The system will be compliant with the ICO and Data Protection guidelines with regard to online safety procedures being maintained at all times.
- 4.1.3 Regular audits and evaluations of the IT network will be carried out, identifying where improvements can be made.
- 4.1.4 TSE staff will be responsible for monitoring IT use.

4.2 Filtering

- 4.2.1 TSE will ensure an appropriate filtering system is used on both the VLE and Discord channels. Filtering reports and logs will be reviewed regularly.
- 4.2.2 Any filtering incidents are examined and action taken and recorded.

4.3 Data Protection

- 4.3.1 Personal data will be recorded, processed, transferred and made available according to the TSE Privacy Notice.
- 4.3.2 A personal data breach (the loss, unauthorised access to, or unauthorised disclosure of personal data) must be reported immediately to contact@thinkspace.ac.uk.
- 4.3.3 Where a breach is likely to result in a risk to individuals' rights and freedoms, TSE will report it to the Information Commissioner's Office within 72 hours of becoming aware of it, as required by UK GDPR, and will inform affected individuals where that risk is high.

4.4 TSE Management and Online Safety

- 4.4.1 TSE's Senior Management are responsible for determining, evaluating and reviewing online safety and the use of IT equipment and facilities by students and staff. The Board of Directors will regularly review online safety and receive reports from Senior Management.

4.5 IT Support Staff

- 4.5.1 Internal IT support staff are responsible for maintaining TSE's web services, IT infrastructure and hardware. IT staff will be aware of current thinking and trends in IT security and ensure that the system is secure. IT staff will ensure systems are not open to abuse or unauthorised external access.
- 4.5.2 IT support staff are responsible for:
 - (a) Defending the network and infrastructure, reviewing activity logs regularly
 - (b) Ensuring that users comply with basic access policies

- (c) Ensuring filtering is robust and regularly checked for penetration to ensure that the risk of staff or students using inappropriate language or behaviours is minimised
- (d) Keeping up to date with current threats and attack trends and taking steps to mitigate these and communicate with the management team
- (e) Reporting to the senior management team any network intrusions or other threats to the network
- (f) Promoting basic cyber security practices within TSE

4.6 All Staff

- 4.6.1 Teaching and support staff are responsible for ensuring that they are aware of the current online safety policy, practices and associated procedures for reporting online safety incidents in line with TSE procedures.
- 4.6.2 All staff will be provided with access to online safety support materials.
- 4.6.3 All staff will ensure that they have read, understood and signed the Staff Contract which contains the Acceptable Use Policy relevant to Internet and computer use.
- 4.6.4 All teaching staff are to be vigilant in monitoring student online behaviour in line with the policy. This may include the use of personal technology, such as cameras or phones, where there is a cause for concern.
- 4.6.5 Staff must promote and reinforce safe online practices when on and off-site, including providing advice to students on how to report incidents.

4.7 Artificial Intelligence (AI) Tools

- 4.7.1 Staff and students must not upload personal data, confidential TSE information, student work or other sensitive material to external AI platforms (for example chatbots, transcription, translation or image-generation services) without prior approval from TSE. Consumer AI tools may store, process and reuse submitted content outside TSE's control, which could breach UK GDPR and the Data Protection Act 2018.
- 4.7.2 Staff using AI tools in teaching, assessment or administrative work must ensure that no student personal data is entered into such tools unless the tool has been approved by TSE for that purpose.
- 4.7.3 The use of AI in academic work is governed by the TSE AI Use Policy, in the postgraduate introduction course on the VLE.

5 Review

- 5.1 This policy will be monitored as part of TSE's annual internal review of student and staff welfare and online safety and security.

Appendix 1: Acceptable Use Policy

Acceptable Internet Use Statement for Students and Staff

In ThinkSpace Education (TSE), students and tutors work in partnership within a learning community. Mutual respect and responsible attitudes to each other are expected, as set out in TSE's student policies.

The web servers, data and computer systems at TSE are the property of TSE and are a resource shared by all students and staff. Web facilities and computer facilities are made available to students to further their education and to staff to enhance their professional activities, including teaching, research, administration and management.

Key Points:

TSE reserves the right to examine or delete any files, including emails, that may be held on its computer system and to monitor or restrict access to any Internet sites visited.

This Acceptable Internet Use Statement is included in the Staff and student contracts respectively.

- (a) All use of TSE web and IT facilities should be appropriate to staff professional activity, student's education, or reasonable personal use
- (b) Activity that threatens the integrity of TSE's ICT systems, or activity that attacks or corrupts other systems, is forbidden
- (c) Users are responsible for all email sent and for contacts made that may result in email being received
- (d) Copyright of materials must be respected
- (e) Use of personal financial gain, gambling or political purposes is forbidden
- (f) Use of the web servers or TSE network to access inappropriate material is forbidden