



ACCEPTABLE USE, E-SAFETY, EMAIL AND SOCIAL MEDIA POLICY

Policy reference UKV-QA-30 | Version 3.0

UK Versity Online Limited | BAC Accredited College | UKPRN 10052768

Policy reference	UKV-QA-30
Version	3.0
Status	Consolidated
Effective date	1 October 2026
Next review	September 2027
Policy owner	Centre Coordinator
Author	Director of Education
Approved by	Principal (Ramanjeet Singh), on behalf of the Academic Board
Approval date	1 October 2026

Acceptable Use, E-Safety, Email and Social Media Policy

UK Versity Online Limited | ATHE 889 | Pearson 07737 | OTHM DC1506132 | Ascentis 3286 | NCFE 8465520 | IFA Direct 283334

Document control

Title	Acceptable Use, E-Safety, Email and Social Media Policy
Reference	UKV-QA-30
Version	3.0
Status	Consolidated
Effective date	1 October 2026
Next review	September 2027 (annual), or earlier if required
Owner	Centre Coordinator
Author	Director of Education
Approval authority	Academic Board, chaired by the Principal (Ramanjeet Singh)
Approval date	1 October 2026
Applies to	All UK Versity staff, tutors, assessors, Internal Quality Assurers, contractors and learners using UK Versity systems or representing UK Versity online
Supersedes	Email Usage and Security Policy QA-178 (August 2014, next review November 2027); Social Media and Professional Representation Policy QA-M120 (November 2014, next review November 2026)
Summary	Sets the rules for safe and responsible use of Moodle, Zoom, email, messaging and social media by UK Versity staff and learners, including e-safety, security and the use of AI tools.

Compliance mapping

BAC College Scheme 2023 standards	2.7; 16.6; 16.9; 26.4
UK Quality Code 2024 (voluntary)	Principle 3
OfS conditions (benchmark only; not OfS registered)	B2 (benchmark)
Awarding organisations	ATHE; Pearson; OTHM; Ascentis; NCFE; IFA Direct
Legislation and regulation	UK GDPR and Data Protection Act 2018; Privacy and Electronic Communications Regulations 2003; Computer Misuse Act 1990; Online Safety Act 2023; Human Rights Act 1998; Equality Act 2010

Version history

Version	Date	Change
1.0	August 2014	First issue (Email Usage and Security Policy QA-178; Social Media Policy QA-M120, November 2014)

Version	Date	Change
3.0	October 2026	Full rebuild: email, social media, acceptable use and e-safety combined for staff and learners; MFA, phishing, AI tools and monitoring notice added; BAC mapping and version control

1. Purpose

UK Versity Online Limited (trading as UK Versity) is a fully online college. Moodle, Zoom, email and messaging are the college's classrooms and offices. This policy sets the rules that keep learners and staff safe online, protect personal data and UK Versity systems, and make sure everyone who represents UK Versity does so accurately and professionally. It meets BAC standards 16.9 (e-safety policy), 16.6 (abusive behaviour including cyberbullying), 26.4 (monitoring online risks) and 2.7 (data security).

2. Scope

This policy applies to:

- all staff, self-employed tutors, assessors, Internal Quality Assurers (IQAs) and contractors (in this policy, "staff");
- all learners;
- all UK Versity systems: Moodle (lms.ukversity.co.uk), Zoom, UK Versity email, Zoho systems, official WhatsApp groups and UK Versity social media accounts;
- personal devices and personal social media where they are used for UK Versity work or study, or where conduct affects UK Versity, its learners or staff.

3. Definitions

- **UK Versity systems:** any account, platform or device provided or managed by UK Versity.
- **Multi-factor authentication (MFA):** a login that needs a second check, such as a code from an app, in addition to a password.
- **Phishing:** a message designed to trick you into revealing passwords or personal data, making a payment or opening a harmful file or link.
- **Public AI tool:** a generative AI service (for example a chatbot) that is not provided by UK Versity under a data processing agreement.

4. Policy statement and principles

1. UK Versity systems are provided for learning, teaching, assessment and college business. Limited personal use by staff is allowed if it does not interfere with work or breach this policy.
2. Everyone is responsible for what they post, send or share using UK Versity systems.
3. Behaviour online must meet the same standards as behaviour in person. Bullying, harassment and discrimination are not tolerated (UKV-QA-26).
4. Personal data is protected under UKV-QA-29 at all times.
5. Safeguarding concerns that arise online are reported under UKV-QA-25 the same day.

5. Acceptable use of Moodle and Zoom

5.1 Everyone

- Use only your own login. Never share your username or password, and never let anyone else submit work or attend a session in your name.
- Do not upload, post or share anything illegal, offensive, discriminatory, sexually explicit, extremist or defamatory, or any malware.
- Do not record, photograph or screenshot live sessions or other people, and do not share session links or recordings outside UK Versity.
- Do not try to access areas, data or accounts you are not authorised to use.

5.2 Learners

- Use a respectful tone in forums, chat and sessions. Disagree with ideas, not people.
- Join live sessions from a suitable place, with a neutral background or background blur if your camera is on.
- Submit only your own work, following UKV-QA-19 Academic Integrity, Plagiarism and Use of AI Policy.
- Report anything that worries you to your tutor, the Student Administrator and Welfare Officer or admin@ukversity.co.uk.

5.3 Staff

- Run live sessions only through UK Versity's Zoom account, using the waiting room and authenticated links. Only staff may share screens.
- Tell learners at the start of each session that it is being recorded and uploaded to Moodle.
- Follow the rules on one-to-one contact with learners under 18 in UKV-QA-25 section 7.
- Moderate chat, forums and breakout rooms, and remove harmful content.

6. E-safety

UK Versity helps learners stay safe online by:

1. covering e-safety at induction on Moodle: protecting personal information, recognising grooming, radicalisation, sextortion, scams and phishing, and how to report concerns;
2. moderating Moodle forums and official WhatsApp groups;
3. keeping live sessions secure (section 5);
4. restricting administrator rights on all platforms to authorised staff, and reviewing platform security settings at least every three months;
5. giving learners information on where to get help, including the Designated Safeguarding Lead, Samaritans (116 123) and, in an emergency, 999.

If you receive threats, requests for images or money, or messages that make you feel unsafe from anyone connected to UK Versity, do not respond or pay. Keep the evidence and report it to the Designated Safeguarding Lead through admin@ukversity.co.uk or 0161 273 4745.

7. Online conduct and cyberbullying

Cyberbullying includes abusive, threatening or humiliating messages, posting or sharing images or personal information about someone without consent, excluding someone from online groups, impersonating

someone, and repeated unwanted contact. It is a disciplinary matter for learners and staff wherever it happens, if it involves UK Versity learners or staff. Reports are dealt with under UKV-QA-26 and, where there is a risk of harm, UKV-QA-25.

8. Email

1. Staff must use their UK Versity email account for all college business and must not use personal email for learner or college data. Learners should use the email address registered at enrolment. Assignments are submitted through Moodle or to learnerwork@ukversity.co.uk where instructed.
2. Email accounts are personal and must not be shared.
3. Sending limits: a maximum of 100 emails per hour per user. Bulk emails must be approved by the Centre Coordinator and sent only through authorised systems.
4. Attachments: a maximum of 20MB per email. Do not attach folders. Large or sensitive files must be shared through approved UK Versity file storage with access restricted to the people who need it.
5. Check recipients before sending. Use blind copy when emailing groups of learners so addresses are not disclosed.
6. **Account lockout.** Repeated failed logins can block an account and may affect email for the whole organisation. If your account is blocked or shows a warning symbol, tell the Centre Coordinator at once, close your email application and wait 15 to 20 minutes before trying again. Do not repeatedly enter or reset your password.
7. Marketing emails are sent only in line with the Privacy and Electronic Communications Regulations 2003 and UKV-QA-02.

9. Passwords, MFA and devices

1. Use a strong, unique password for each UK Versity account. Do not reuse passwords from personal accounts.
2. MFA must be switched on for UK Versity email, Zoho and all administrator accounts, and for Moodle staff accounts where available.
3. Lock your screen whenever you leave your device.
4. **Personal devices.** Staff may use a personal device for UK Versity work only if it has a supported, updated operating system, a screen lock, and up-to-date security software, and is not shared with other people while logged in. Learner data must not be downloaded to or stored on personal devices, personal email or personal cloud storage.
5. Report a lost or stolen device used for UK Versity work to the Centre Coordinator and the Data Protection Lead immediately, so that access can be removed.

10. Phishing and cyber security

1. Do not click links or open attachments you are not expecting. Check the sender's address carefully.
2. Never give your password in response to an email, message or call. UK Versity will never ask for it.
3. Be suspicious of urgent requests to change bank details or make payments. The Financial Controller confirms any change to payment details by telephone using a known number before acting.
4. Review cookie settings on websites and do not allow unnecessary tracking.
5. Report suspected phishing or a suspected security incident to the Centre Coordinator immediately. If personal data may be affected, the Data Protection Lead handles it as a breach under UKV-QA-29.

11. Use of AI tools with learner or college data

1. Never paste, upload or type personal data (such as learner names, ID numbers, contact details, assessment feedback linked to a named learner, or learner work) into a public AI tool.
2. AI and plagiarism screening of learner work is carried out only through the tools approved by UK Versity (currently GPTZero), under a data processing agreement.
3. Staff may use AI tools to help prepare general teaching materials, provided no personal or confidential data is used and the output is checked for accuracy before use.
4. A new AI tool that processes personal data may only be used after the Data Protection Lead has approved it and completed a data protection impact assessment.
5. Learners' use of AI in their own work is governed by UKV-QA-19.

12. Social media

12.1 Official UK Versity accounts

1. Only staff authorised by the Principal may post on or administer official UK Versity social media accounts. Administrator access is removed when a person leaves.
2. Posts must be accurate and follow UKV-QA-02 Public Information, Marketing and Agents Policy. Qualification titles, awarding organisation names, levels and accreditation must be stated correctly. UK Versity is described as "accredited by the British Accreditation Council as a College".
3. Learner names, images, work or testimonials are posted only with the learner's written consent.
4. Official accounts are monitored, and harmful or extremist content is removed and reported.

12.2 Staff personal and professional profiles

1. Where staff keep a professional networking profile (for example LinkedIn), their current job title, the company name "UK Versity Online Limited" and start date must be accurate. New staff update their profile within one week of starting.
2. Staff must not post confidential information, learner information, or negative, defamatory or misleading statements about UK Versity, colleagues or learners.
3. Staff must not use UK Versity's name or branding in personal posts unrelated to work.
4. Staff may be asked to share official UK Versity posts. Only official content may be shared, never personal or sensitive data.
5. Staff must not connect with, follow or message learners on personal social media accounts (UKV-QA-25).

12.3 Learners

Learners must not post content about other learners or staff, recordings of sessions, or course materials on social media or file-sharing sites. Sharing assessment material or answers is academic misconduct under UKV-QA-19.

13. Monitoring notice

UK Versity may monitor and access the use of its systems, including email, Moodle activity logs, Zoom records and official messaging groups, to protect systems and data, keep learners safe, verify authenticity of learner work, investigate suspected breaches of policy or law, and meet awarding organisation requirements. Monitoring is lawful, proportionate and carried out only by authorised staff under UK GDPR, the Data Protection Act 2018 and the Human Rights Act 1998. UK Versity does not routinely read the content of

individual emails. Staff and learners should not expect privacy in their use of UK Versity systems for college business.

14. Breaches of this policy

Breaches are dealt with according to seriousness:

- **Staff:** informal discussion, suspension of system access, the disciplinary procedure and, for serious breaches (such as sharing learner data or credentials, or cyberbullying), dismissal or termination of contract.
- **Learners:** a warning, restricted access to forums or groups, action under UKV-QA-19 or UKV-QA-20, or suspension or withdrawal from the programme.
- Illegal activity is reported to the police. Data breaches are handled under UKV-QA-29.

All staff confirm at induction that they have read and will follow this policy. Learners agree to it as part of the Learner Agreement (UKV-QA-10).

15. Roles and responsibilities

Role	Responsibility
Centre Coordinator	Owns this policy; manages system accounts, MFA and lockouts; handles security incidents; approves bulk emails
Principal and Director of Education (Data Protection Lead)	Authorises social media administrators; approves AI tools and DPIAs; manages data breaches
Course Coordinator	Manages Moodle permissions and moderation; reviews platform security settings at least every three months
Designated Safeguarding Lead	Responds to online safeguarding and e-safety concerns
Financial Controller	Verifies any change to payment details
Tutors	Run secure live sessions; moderate chat and forums; model good online conduct
All staff	Follow this policy; report incidents and phishing immediately
Learners	Use UK Versity systems safely and respectfully; protect their login; report concerns

16. Related policies and legislation

- UKV-QA-02 Public Information, Marketing and Agents Policy
- UKV-QA-10 Learner Agreement
- UKV-QA-13 Online and Distance Learning and Course Materials Policy
- UKV-QA-19 Academic Integrity, Plagiarism and Use of AI Policy
- UKV-QA-20 Malpractice and Maladministration Policy and Procedure
- UKV-QA-25 Safeguarding and Prevent Policy
- UKV-QA-26 Equality, Diversity, Inclusion and Anti-Harassment Policy
- UKV-QA-29 Data Protection and Records Retention Policy
- UK GDPR and Data Protection Act 2018
- Privacy and Electronic Communications Regulations 2003

- Computer Misuse Act 1990
- Online Safety Act 2023
- Human Rights Act 1998
- Equality Act 2010
- BAC College Scheme 2023, standards 2.7, 16.6, 16.9 and 26.4

17. Monitoring and review

The Centre Coordinator keeps a log of security incidents, phishing reports, account lockouts and policy breaches. The Course Coordinator records the three-monthly platform security reviews. A summary, with e-safety incidents reported by the Designated Safeguarding Lead, goes to the Academic Board at least annually.

This policy is reviewed at least annually, and earlier if legislation, technology used by UK Versity, awarding organisation requirements, BAC standards, an inspection or EQA action, or a significant incident requires it. Each version is recorded in the Policy Register (UKV-QA-REG v3.0). Incident logs are kept for 3 years, and records linked to a data breach or disciplinary case are kept as set out in UKV-QA-29.

Approval and review

Stage	Name and role	Date
Prepared by	Director of Education	30 September 2026
Checked by (policy owner)	Centre Coordinator	30 September 2026
Approved by	Ramanjeet Singh, Principal and Director of Education, on behalf of the Academic Board	1 October 2026
Next review due	Quality Manager (Shazia Khan) to schedule through the Policy Register UKV-QA-REG	September 2027