

Social Media, AI & Digital Communication Policy

1. Purpose of the Policy

This Social Media & Digital Communication Policy sets out clear expectations for the safe, professional, and appropriate use of social media, messaging apps, and digital communication tools by staff, volunteers, and contractors working for IP / Europa School of English.

The policy exists to:

- Safeguard students (particularly those under 18)
- Protect staff from misunderstandings, allegations, or inappropriate conduct
- Maintain professional boundaries
- Protect the reputation of the school

This policy should be read in conjunction with the Adult Behaviour Policy (Code of Conduct) and all safeguarding-related policies.

2. Scope

This policy applies to:

- All staff, volunteers, and contractors (paid or unpaid)
- All forms of digital communication, including but not limited to:
 - Social media platforms (e.g. Instagram, Facebook, TikTok, X)
 - Messaging apps (e.g. WhatsApp)
 - Email
 - Online forums, comments, and direct messages

It applies both during employment and where online behaviour may reasonably be linked to the school or affect its reputation.

3. Professional Conduct Online

Staff are expected to act as professional role models at all times.

- Online behaviour should reflect the same standards as face-to-face conduct
- Content must not bring the school into disrepute

- Staff must not post discriminatory, offensive, sexually suggestive, aggressive, or unlawful material
- Staff should exercise judgement regarding personal posts that may affect their professional role

Staff should assume that any online content may become public, even if privacy settings are enabled.

4. Personal Social Media Accounts

- Staff must keep personal social media accounts private wherever possible
- Staff must not identify themselves as speaking on behalf of the school unless authorised
- Staff must not post confidential information relating to students, staff, or school operations

Students under 18

- Staff must not accept or send friend / follower / contact requests
- Staff must have no private online contact with students or former students under 18

Adult students (18+)

- Staff should maintain professional boundaries
- Staff should not engage in private messaging or social interaction beyond course-related matters
- Any communication should be respectful, appropriate, and transparent

5. Use of WhatsApp

Parents are informed of the potential use of WhatsApp in our organisation and are asked to provide or decline to give consent via our parental consent form.

Permitted Use

WhatsApp groups may be used for operational and safeguarding purposes only under the following conditions:

- Announcements-only group
- Groups do not include any students who have not had permission via the parental consent form
- Participants cannot reply
- Student participants mobile numbers cannot be seen by others. Only staff numbers are visible or any people added to sub groups (Group Leaders only)
- Groups can be created for:

- Course-related information
- Timetables and schedules
- Excursion details
- Emergency or welfare updates
- Groups may include students and/or group leaders
- Groups should not include any students under the age of 13 yrs
- Groups must not contain any persons from outside the organisation.

Mandatory Safeguarding Conditions

- A designated member of staff must be included in the group
- This staff member must be an admin
- The staff member is responsible for monitoring:
 - Tone and content of messages
 - Appropriate behaviour
 - Safeguarding concerns
- Groups must be used only for professional purposes
- All staff members in the group must also take responsibility for monitoring content and tone.

Groups must be set up so that only staff members can post. Staff must post information in a responsible, professional and polite manner at all times.

Prohibited Use

- No private one-to-one WhatsApp chats with students
- No informal, social, or personal conversations
- No sharing of personal contact details

Group Closure

- WhatsApp groups must be deleted as soon as the course or programme ends

6. Photos, Videos, and Media Content

Parents are asked for their consent for their student to be featured on photos or video content for our in house social media content as part of our parental consent form.

- Staff must never upload photos or videos of students to personal accounts
- All student media content must:
 - Be taken using school-approved devices where possible
 - Be uploaded only to official school platforms

- Have the appropriate parental / student consent

Screenshots of WhatsApp conversations or student messages must never be shared externally.

7. Direct Messaging & Private Contact

- Staff must not communicate with students via personal accounts
- All communication must remain:
 - Professional
 - Necessary
 - Transparent

Staff should always consider how a message could be perceived if reviewed by parents, managers, or safeguarding authorities.

8. Confidentiality & Data Protection

- Personal data must be handled in line with GDPR
- Student contact details must not be stored on personal devices unnecessarily
- Devices should be secured with passwords and not shared

Any data breach or accidental disclosure must be reported immediately to the Operations Manager.

9. Monitoring & Reporting Concerns

Staff must report:

- Inappropriate messages or online behaviour
- Safeguarding concerns arising from digital communication
- Any accidental breach of this policy

Concerns should be reported to the safeguarding team in line with the Whistleblowing Policy.

10. Use of Artificial Intelligence (AI)

The school recognises that Artificial Intelligence (AI) tools (e.g. text generators, image generators, translation tools, chatbots, and automated content platforms) are increasingly

used in education and communication. AI may be used appropriately and responsibly in line with professional standards, safeguarding expectations, and data protection legislation.

Permitted Use of AI

Staff may use AI tools for legitimate professional purposes, including:

- Drafting or supporting lesson planning materials
- Creating teaching resources or activities
- Improving clarity or level-appropriateness of written content
- Supporting administrative tasks
- Assisting with marketing content only when authorised and reviewed by management

All AI-generated content must be:

- Reviewed and edited by a member of staff
- Accurate, appropriate, and suitable for the intended audience
- Aligned with the school's values, safeguarding duties, and academic integrity

Prohibited Use of AI

Staff must not:

- Input personal data relating to students, staff, or group leaders into AI tools
- Use AI to communicate directly with students (e.g. automated replies or chatbots)
- Use AI to generate private messages to students
- Use AI to bypass professional judgement or safeguarding responsibilities
- Use AI to create misleading, false, discriminatory, or inappropriate content

AI tools must never replace direct professional responsibility or supervision.

Safeguarding and Confidentiality

- No identifying information (names, contact details, medical information, behaviour records, safeguarding concerns) may be entered into AI systems
- Staff must assume that any data entered into AI tools may be stored externally
- Any accidental data entry or suspected breach must be reported immediately to the Operations Manager

Transparency and Accountability

- Staff remain fully accountable for all content produced with AI assistance
- Where appropriate, staff should be transparent with managers about the use of AI in their work
- Students must not be led to believe that AI-generated content replaces teacher input or assessment

11. Breaches of the Policy

Failure to comply with this policy may result in:

- Disciplinary action
- Removal from duties
- Termination of employment

Serious breaches involving safeguarding may be referred to external authorities.

12. Professional Judgement

If a situation arises that is not explicitly covered by this policy:

- Staff must act in the best interests of student safety
- Actions must be proportionate, appropriate, and recorded
- The situation must be reported to a line manager immediately