POLICY STATEMENT

Social Media

VERSION NUMBER:	**1.0**
THIS VERSION:	**1.0**
PREVIOUS VERSION:	**-**
ORIGINAL VERSION:	**-**
OWNER:	**GROUP DIRECTOR OF MARKETING & COMMUNICATIONS**
TYPE OF PAPER:	**POLICY STATEMENT**
TOPIC AREA:	**SOCIAL MEDIA**
DOCUMENT REF:	**PS.MARKETING.SOCIALMEDIA**

A. AIM & PURPOSE

The aim of this policy is to provide a group social media policy for the International Schools Partnership that regions and schools can adopt according to their local legislation to enable staff to enjoy the benefits of social networking while understanding the standards of conduct expected by the group. It is intended to minimise the risks that can impact on the wellbeing of staff, students and the reputation of the group and all of the schools within.

The purpose of this policy is to encourage good practice, to protect the company, the schools and staff, and to promote the effective use of social media as part of the group's activities.

- This policy covers personal and professional use of social media and aims to encourage its safe use by the school and its staff.
- The policy applies regardless of whether the social media is accessed using the company's IT facilities and equipment, or equipment belonging to members of staff.
- Personal communications via social media accounts that are likely to have a negative impact on professional standards or the school's reputation are within the scope of this policy.
- This policy covers all individuals working at all levels and grades, including full-time and part-time staff, fixed-term staff and agency workers.

B. SCOPE

This Policy Statement is **mandatory** for all Schools in the Group, and all parts of the business including ISP Central Team.

C. DEFINITIONS

Group: ISP and any subsidiary or related group company.
Regional Managing Directors: the managers responsible for each Region within the ISP Group.
ISP: International Schools Partnership Limited.
ISP Board: The board of directors of ISP. This is the Group's strategic board.
ISP Team: Any member of Staff not solely focused on the delivery of services at a particular School. This includes Staff based in ISP's London office and in any of its regional support teams.

SMT: The ISP Senior Management Team.
Policy Application Notes: Notes setting out the legal and regulatory requirements relevant to implementing the key principles of this Policy Statement, which must be fully up to date and compliant with the applicable laws, regulation/s, local child safeguarding procedures, and best practice in the relevant Region.
Region: Europe, Middle East, Mexico & Central America, Southeast Asia, South America and the USA.
School: Any school which is part of the ISP Group.
Staff: any person employed or engaged by ISP, whether ISP Central Office Staff, School Staff, or Regional Office Staff.
Student: Any child or young adult enrolled on a course of study at a School in the Group.

D. ROLES AND RESPONSIBILTIES

The **ISP Board** has overall responsibility for ensuring that this Policy Statement complies with our legal and ethical obligations, and that those under ISP's control comply with it.
The **Policy Owner** has delegated responsibility for oversight of the implementation of this Policy Statement and is responsible for appropriate reporting under this Policy Statement to the ISP Board, which shall be a minimum of once a year.
The Policy Owner on behalf of the ISP Board will monitor the effectiveness of this Policy Statement through regular review, and via an internal audit process. This will include an annual review of this Policy Statement.
The **ISP SMT** is responsible for ensuring the implementation of this Policy across the Group and delegates day to day responsibility in each Region to the **Regional Managing Director**, who in turn are responsible for:

- Developing Policy Application Notes, which are fully compliant with this Policy Statement and approved by the Policy Owner;
- Keeping the Policy Application Notes under regular review, and communicating any updates to those to whom this Policy applies;
- Ensuring each Region and School has its own policy, which is fully compliant with this Policy Statement and the Policy Application Notes;
- Monitoring the implementation and effectiveness of each School's policy.

All Staff in roles that may involve official use of social media for ISP must ensure that they read, understand, and comply with this Policy Statement, and the relevant supporting Policy Application Notes and School policies. The following roles are automatically deemed to involve social media usage in an official capacity:

- Central Marketing, Admissions and Communications team members;
- Central Human Resources team members;
- Regional Marketing, Admissions and Communications team members;
- School Head Teachers;
- School Senior Leadership Team members;
- School Marketing, Admissions and Communications team members;
- School Human Resources team members.

All Staff are required to avoid any activity that might lead to, or suggest, a breach of this Policy Statement. If anyone is unclear on any aspect relating to the application of this Policy Statement, they should seek guidance from the Regional Managing Director or the Policy Owner.
Furthermore, **all Staff** are required to:

- be aware of their online reputation and recognise that their online activity can be seen by others including parents, students and colleagues on social media ensure that any use of social media is carried out in line with this policy and other relevant policies, i.e. those of the employer

- be aware that any excessive use of social media in the company or school may result in disciplinary action
- be responsible for their words and actions in an online environment. They are therefore advised to consider whether any comment, photograph or video that they are about to post on a social networking site is something that they want colleagues, students, parents, other staff of the group, or even future employers, to read. If in doubt, do not post it!

Managers are responsible for:

- addressing any concerns and/or questions staff may have on the use of social media
- operating within the boundaries of this policy and ensuring that all staff understand the standards of behaviour expected of them.

Marketing & Communications is responsible for:

- giving specialist advice on the use of social media
- implementing and reviewing this policy.

E. KEY POLICY PRINCIPLES

The International Schools Partnership recognises and embraces the numerous benefits and opportunities that social media offers. While staff are encouraged to engage, collaborate and innovate through social media, they should also be aware that there are some associated risks, especially around issues of safeguarding, bullying and personal reputation.

1. Definition of social media

Social media is a broad term for any kind of online platform which enables people to directly interact with each other. It allows people to share information, ideas and views. Examples of social media include blogs, Facebook, LinkedIn, Twitter, Google+, Instagram, Flickr, Vimeo and YouTube.

2. Acceptable use

Staff should be aware that content uploaded to social media is not private. Even if you restrict it to 'friends', there is still capacity for it to be re-posted or distributed beyond the intended recipients. Therefore, staff using social media should conduct themselves with professionalism, care and respect.

Staff should not upload any content on to social media sites that:

- is confidential to the company, schools or its staff
- amounts to bullying
- amounts to unlawful discrimination, harassment or victimisation
- brings the company or schools into disrepute
- contains lewd, sexually explicit, threatening or similarly inappropriate or offensive comments, images or video clips
- undermines the reputation of the company, schools and/or individuals
- is defamatory or knowingly false
- breaches copyright
- is in any other way unlawful.

Staff in the group and the schools should be aware of both professional and social boundaries and should not therefore accept or invite 'friend' requests from students or ex-students under the age of 18, or from parents on their personal social media accounts such as Facebook, Twitter, Instagram etc. All communication with parents via social media should be through the group's or schools' social media accounts.

Staff should note that the use of social media accounts during working hours (outside of sanctioned official use on behalf of the company and/or the schools) is not permitted.

3. Safeguarding

The use of social networking sites introduces a range of potential safeguarding risks to children and young people. Potential risks can include, but are not limited to:

- online bullying
- grooming, exploitation or stalking
- exposure to inappropriate material or hateful language
- encouraging violent behaviour, self-harm or risk taking.

In order to mitigate these risks, there are steps you can take to promote safety on-line:

- You should not use any information in an attempt to locate or meet a child.
- Ensure that any messages, photos or information comply with existing policies.

Further advice can be found in the appendix below. Please ensure you consult this guidance thoroughly when using social media both for professional and personal use.

4. Reporting safeguarding concerns

- Any content or online activity which raises a safeguarding concern must be reported to the **Group Head of Safeguarding** and/or the **Designated Safeguarding Lead (DSL)** in the school where the concern has been raised.
- Any online concerns should be reported as soon as identified as urgent steps may need to be taken to support the child.
- With regard to personal safeguarding, you should report any harassment or abuse you receive online while using your work accounts.

5. Reporting, responding and recording cyberbullying incidents

- Staff should never engage with cyberbullying incidents. If in the course of your employment with this company or any school within the group, you discover a website or social media site containing inaccurate, inappropriate or inflammatory written material relating to you, or images of you which have been taken and/or which are being used without your permission, you should immediately report this to a **senior manager and Human Resources**.
- Staff should keep any records of the abuse such as text, emails, voicemail, website or social media. If appropriate, screen prints of messages or web pages could be taken and the time, date and address of site should be recorded.

6. Action by Group: inappropriate use of social media

- Following a report of inappropriate use of social media, the senior manager will conduct a prompt investigation involving Human Resources.
- If in the course of the investigation, it is found that a staff member submitted the material to the site in question, that staff member will be disciplined in line with the group's disciplinary policy. If a student is found to have submitted the material to the site in question, the student will be disciplined in line with the school's behaviour policy.
- The senior manager, where appropriate, will approach the social media or website hosts to ensure the material is either amended or removed as a matter of urgency, i.e. within

24 hours. If the social media or website requires the individual who is complaining to do so personally, the group will give their full support and assistance.

- Checks will be carried out to ensure that the requested amendments or removals are made. If the website(s) does not co-operate, the senior manager will contact the internet service provider as the the internet service provider has the ability to block access to certain sites and, in exceptional circumstances, can close down a website or social media account.
- If the material is threatening and/or intimidating, senior management will, with the member of staff's consent, report the matter to the police.
- The member of staff will be offered full support and appropriate stress counselling.

7. Breaches of this policy

- Any member of staff suspected of committing a breach of this policy (or if complaints are received about unacceptable use of social networking that has potentially breached this policy) will be investigated in accordance with the group or school's disciplinary procedure. The member of staff will be expected to co-operate with the school's investigation which may involve:
  - handing over relevant passwords and login details
  - printing a copy or obtaining a screenshot of the alleged unacceptable content
  - determining that the responsibility or source of the content was in fact the member ofstaff
- The seriousness of the breach will be considered including the nature of the content, how long the content remained visible on the social media site, the potential for recirculation by others and the impact on the group or school, or the individuals concerned.
- Staff should be aware that actions online can be in breach of the harassment/safeguarding/ acceptable use/equality policies and any online breaches of these policies may also be treated as conduct issues in accordance with the disciplinary procedure.
- If the outcome of an investigation leads to disciplinary action, the consequences will be dealt with in accordance with the appropriate procedures. Serious breaches could result in the dismissal of the staff.
- Where conduct is considered to be unlawful, the group or school will report the matter to the police and other external agencies.

8. Monitoring and review

- If the manager reasonably believes that an staff has breached this policy, from time to time the group or school will monitor or record communications that are sent or received from within the group or school's network.
- This policy will be reviewed on a yearly basis and, in accordance with the following, on an as-and-when-required basis:
  - legislative changes
  - good practice guidance
  - case law
  - significant incidents reported.
- This policy does not form part of any staff's contract of employment and may also be amended from time to time by the group.

9. Legislation

- Acceptable use of social networking must comply with UK law. In applying this policy, the group will adhere to its rights, responsibilities and duties in accordance with the following:

  - Regulation of Investigatory Powers Act 2000
  - General Data Protection Regulations (GDPR) 2018
  - The Human Rights Act 1998
  - The Equality Act 2010
  - The Defamation Act 2013

10. Conclusion

- The internet is a fast-moving technology and it is impossible to cover all circumstances or emerging media - the principles set out in this policy must be followed irrespective of the medium.
- When using social media, staff should be aware of the potential impact on themselves and the employer, whether for work-related or personal use; whether during working hours or otherwise; or whether social media is accessed using the employer's equipment or using the staff's equipment.
- Staff should use discretion and common sense when engaging in online communication. There are some general rules and best practice in the appendix which staff should read and use as a guide for all social media activity.

F. CROSS REFERRED POLICIES

This Policy Statement should be read alongside the following ISP Policy Statements:

- Safeguarding Policy
- Acceptable Use
- Data Protection
- Disciplinary
- Code of Conduct

Appendix

Guidance - Responsible use of social media

Remember that anything you post online is not really private. Below are some common-sense guidelines and recommendations that staff are urged to follow to ensure responsible, professional and safe use of social media.

- Do not add students as friends or contacts in your social media accounts.
- Follow this social media policy.
- Never post any information which can be used to identify a student. This includes:
    - posting snapshot images or recordings of an online lesson that display not only children's faces but their full names and their homes.
    - Even a piece which shows children explaining their work needs careful consideration on how it is presented.
    - Images of students with names on their school clothing.
    - For all posts that include students, if posting their names, **only use first names**.
- Always maintain professional boundaries. Do not engage in discussion with students online unless through official group or school accounts.
- Think about the potential risks: professional boundaries of adding parents to your private social media accounts (refer to policy).
- Consider using an alternative name on sites like Facebook to make it harder for students to find you. For example, some staff members use their partner's surname online but their own surname in school.
- Never post anything that is offensive or aggressive, even if you are very angry or upset. It can easily be taken out of context.
- Remember humour is relative. For example, posting images and/or text about a recent night out may be deemed inappropriate. Likewise, a few 'light-hearted' comments and/or images about colleagues or students may not be perceived as such by either subject(s) of the humour or the employer. **The guiding rule is:** if in doubt, don't post it!
- Make sure you regularly check and refresh your site page to ensure it is free of any inappropriate comments and/or images.
- If you are tagged in something in Facebook that you consider inappropriate, use the remove tag feature to untag yourself (for details on how to do this, refer to the Facebook help centre).
- Be cautious of accepting 'friend requests' from people you do not really know. Simply being a 'friend' of your own Facebook friend does not mean that they should automatically be given access to your information.
- Review your profile information and settings on Facebook, Twitter and other sites to ensure it is appropriate as it may be accessed by others such as colleagues, students, parents and potential employers.
- Check your privacy and security settings regularly, and keep your date of birth and home address to yourself. Identity theft is a growing crime and this kind of information could be used to gain access to your bank or credit card account.
- If you feel dissatisfied and wish to rant about work, teaching, politics and life in general, consider doing so anonymously, through a networking account or blog which cannot be attributed to you. Check that anything that you post does not identify you, your school, students or parents.
- Ensure that any comments and/or images could not be deemed defamatory or in breach of copyright legislation.
- Do not use social media in any way to attack or abuse colleagues or air any other internal grievances.
- Do not post derogatory, defamatory, offensive, harassing or discriminatory content.
- Do not engage in any conduct (using personal insults, obscenities) which would not be acceptable in the workplace.
- Do not use social media to 'whistleblow' – raise concerns through the proper channels which would entitle you to legal protection (Public Interest Disclosure Act 1998).