includEd Learning

Independent Specialist Education Provider

SOCIAL MEDIA POLICY

Contents

➔ 1. Statement of Intent

IncludEd Learning understands that social media is a growing part of life outside of school. We have a responsibility to safeguard our students against potential dangers when accessing the internet at school, and to educate our students about how to protect themselves online when outside of school.

We are committed to:

- Encouraging the responsible use of social media by all staff, parents and students in support of the school's mission, values and objectives.
- Protecting our students from the dangers of social media.
- Preventing and avoiding damage to the reputation of the school through irresponsible use of social media.
- Protecting our staff from cyber bullying and potentially career damaging behaviour.
- Arranging e-safety meetings for parents.

➔ 2. Legal Framework

This policy has due regard to legislation and guidance including, but not limited to, the following:

- The General Data Protection Regulation (GDPR)
- DfE (2018) 'Data protection: a tool kit for schools'
- The Data Protection Act 2018

This policy will be implemented in accordance with the following school policies and documents:

- Acceptable Use Policy
- Staff Handbook
- E-Safety Policy
- Data Protection Policy
- Complaints Procedures Policy
- Anti-Bullying Policy
- Allegations of Abuse Against Staff Policy

➔ 3. Roles and Responsibilities

The Head of Centre is responsible for:

- The overall implementation of this policy and ensuring that all staff, parents and students are aware of their responsibilities in relation to social media use.
- Promoting safer working practices and standards with regards to the use of social media.
- Establishing clear expectations of behaviour for social media use.
- Ensuring that this policy, as written, does not discriminate on any grounds, including, but not limited to: ethnicity/national origin, culture, religion, gender, disability or sexual orientation.
- In conjunction with the Advisory Panel, handling complaints regarding this policy and its provisions in line with the school's Complaints Procedures Policy.
- Implementing appropriate sanctions and disciplinary methods where there is a breach of this policy.
- Taking steps to minimise the amount of misplaced or malicious allegations in relation to social media use.
- Working alongside Smoothwall to ensure appropriate security measures are implemented and compliance with the GDPR.

Staff members are responsible for:

- Adhering to the principles outlined in this policy and the Acceptable Use Policy.
- Ensuring students adhere to the principles outlined in this policy and that it is implemented fairly and consistently in the classroom.
- Reporting any social media misuse by staff, students or parents to the Head of Centre and DSL immediately.
- Attending any training on social media use offered by the school.

Parents are responsible for:

- Adhering to the principles outlined in this policy.
- Taking appropriate responsibility for their use of social media and the influence on their children at home.
- Promoting safe social media behaviour for both themselves and their children.
- Attending e-safety meetings held by the school wherever possible.

Students are responsible for:

- Adhering to the principles outlined in this policy.
- Ensuring they understand how to use social media appropriately and stay safe online.

➔ 4. Definitions

For the purpose of this policy, the school defines **"social media"** as any online platform that offers real-time interaction between the user and other individuals or groups including, but not limited to, the following:

- Blogs
- Online discussion forums, such as netmums.com
- Collaborative spaces, such as Facebook/Instagram/SnapChat
- Media-sharing devices, such as YouTube
- Micro-blogging' applications, such as Twitter

- For the purpose of this policy, **"cyber bullying"** is defined as any social media or communication technology intentionally used to bully an individual or group, including the posting or sharing of messages, images or videos.

- For the purpose of this policy, **"members of the school community"** are defined as any teacher, member of support staff, student, parent of a student, Advisory Panel member or ex-student.

➔ 5. Data Protection Principles

- The school will obtain consent from students and parents on joining the school which will confirm whether or not consent is given for posting images and videos of a student on social media platforms. The consent will be valid for the student's stay at school. Parents have the right to withdraw/give consent as they wish.

- A record of consent is maintained, which details the pupils for whom consent has been provided. The is responsible for ensuring this consent record remains up-to-date.

- Where a student is assessed by the school to have the competence to understand what they are consenting to, the school will obtain consent directly from that student; otherwise, consent is obtained from whoever holds parental responsibility for the child.

- Parents and students are able to withdraw or amend their consent at any time. To do so, parents and students must inform the school in writing.

- Consent can be provided for certain principles only, for example only images of a student are permitted to be posted, and not videos. This will be made explicitly clear on the consent form provided.

- Where parents or students withdraw or amend their consent, it will not affect the processing of any images or videos prior to when consent was withdrawn or amended. Processing will cease in line with parents' and students' requirements following this.

- Wherever it is reasonably practicable to do so, the school will take measures to remove any posts before consent was withdrawn or amended, such as removing an image from a social media site.

- The school will only post images and videos of students for whom consent has been received.

- Only school-owned devices will be used to take images and videos of the school community, which have been pre-approved by the Head of Centre for use.

- When posting images and videos of students, the school will apply data minimisation techniques, such as pseudonymisation (blurring a photograph), to reduce the risk of a student being identified.

- The school will not post students' personal details on social media platforms.

- Students' full names will never be used alongside any videos or images in which they are present.

- Only appropriate images and videos of students will be posted in which they are suitably dressed, i.e. it would not be suitable to display an image of a student in swimwear.

- When posting on social media, the school will use group or class images or videos with general labels, e.g. 'sports day'.

- Before posting on social media, staff will:

➔ Refer to the consent record log to ensure consent has been received for that student and for the exact processing activities required.

➔ Ensure that there is no additional identifying information relating to a student.

- Any breaches of the data protection principles will be handled in accordance with the school's data policies.

- Consent provided for the use of images and videos only applies to school accounts – staff, students and parents are not permitted to post any imagery or videos on personal accounts.

-

➔ 6. Social Media Use - Staff

School accounts

- School social media passwords are kept securely; these are not shared unless otherwise permitted by the Head of Centre.
- Staff will ensure any posts are positive in nature and relevant to students, the work of staff, the school or any achievements.
- Staff will adhere to the data protection principles outlined in section 4 of this policy at all times.
- Staff will not post any content online which is damaging to the school or any of its staff or students.
- If inappropriate content is accessed online, a report form will be completed and passed on to the Head of Centre. The Head of Centre and the DSL retain the right to monitor staff members' internet usage in line with the school's Data Management policies.

Personal accounts

- Staff members will not access social media platforms during lesson times.
- Staff members will not use any school-owned mobile devices to access personal accounts, unless it is beneficial to the material being taught – prior permission will be sought from the Head of Centre.
- Staff members are permitted to use social media during break times.
- Staff will avoid using social media in front of students.
- Staff will not "friend" or otherwise contact students or parents through their personal social media accounts.
- If students or parents attempt to "friend" a staff member they will report this to the Head of Centre.
- Staff members will not provide their home address, phone number, mobile number, social networking details or email addresses to students or parents – any contact with students or parents will be done through authorised school contact channels.
- Staff members will ensure the necessary privacy controls are applied to personal accounts.
- Staff members will avoid identifying themselves as an employee of IncludEd Learning on their personal social media accounts.

- No staff member will post any content online that is damaging to the school or any of its staff or students.
- Where staff members use social media in a personal capacity, they will ensure it is clear that views are personal and are not that of IncludEd Learning.
- Staff members will not post any information which could identify a student, class or the school – this includes any images, videos and personal information.
- Staff will not take any posts, images or videos from social media that belong to the school for their own personal use.
- Staff members will not post anonymously or under an alias to evade the guidance given in this policy.
- Breaches of this policy by members of staff will be taken seriously, and in the event of illegal, defamatory or discriminatory content, could lead to prosecution, disciplinary action or dismissal.
- Members of staff will be aware that if their out-of-work activity brings the school into disrepute, disciplinary action will be taken.
- Members of staff will regularly check their online presence for negative content via search engines.
- Attempts to bully, coerce or manipulate members of the school community via social media by members of staff will be dealt with as a disciplinary matter.
- Members of staff will not leave a computer or other device logged in when away from their desk or save passwords.
- Staff members will use their school email address for school business and personal email address for their private correspondence; the two should not be mixed.

➔ 7. Social Media Use - Students and Parents

- Students will not access social media during lesson time, unless it is part of a curriculum activity.
- Students and parents will not attempt to “friend” or otherwise contact members of staff through their personal social media accounts. Students and parents are only permitted to be affiliates of school social media accounts.
- Where a student or parent attempts to “friend” a staff member on their personal account, it will be reported to the Head of Centre/DSL.
- Students and parents will not post anonymously or under an alias to evade the guidance given in this policy.
- Students and parents will not post any content online which is damaging to the school or any of its staff or students.
- Students are instructed not to sign up to any social media sites that have an age restriction above the pupil’s age.
- If inappropriate content is accessed online on school premises, it will be reported to a teacher.
- Students are not permitted to use the school’s WiFi network to access any social media platforms.
- Parents are not permitted to use the school’s WiFi network to access any social media platforms on personal devices.
- Breaches of this policy will be taken seriously, and in the event of illegal, defamatory or discriminatory content could lead to prosecution, or exclusion.

➔ 8. Blocked Content

In accordance with the school's Data Management Policy, the school installs firewalls on the school's network to prevent access to certain websites. The following social media websites are not accessible on the school's network:

- Twitter
- Facebook
- Instagram
- Snapchat

- Attempts made to circumvent the network's firewalls will result in a ban from using school computing equipment, other than with close supervision.
- Inappropriate content accessed on the school's computers will be reported to the Head of Centre so that the site can be blocked.
- The Head of Centre retains the right to monitor staff and student access to websites when using the school's network and on school-owned devices.
- Requests may be made to access erroneously blocked content by submitting a blocked content access form which will be approved by the Head of Centre.

➔ 9. Cyberbullying

Cyberbullying incidents are taken seriously at IncludEd Learning. Any reports of cyberbullying on social media platforms by students will be handled in accordance with the Anti-Bullying Policy.

- Allegations of cyberbullying from staff members will be handled in accordance with the Allegations of Abuse Against Staff Policy.
- Staff members will not respond or retaliate to cyber bullying incidents. Incidents will be reported as inappropriate, and support will be sought from the headteacher.
- Evidence from the incident will be saved, including screen prints of messages or web pages, and the time and date of the incident.
- Where the perpetrator is a current student or colleague, most incidents can be handled through the school's own disciplinary procedures.
- Where the perpetrator is an adult, in nearly all cases, a member of the SLT will invite the victim to a meeting to address their concerns. Where appropriate, the perpetrator will be asked to remove the offensive content.
- If the perpetrator refuses to comply, it is up to the school to decide what to do next. This could include contacting the internet service provider in question through their reporting mechanisms, if the offensive content breaches their terms and conditions.
- If the material is threatening, abusive, sexist, of a sexual nature or constitutes a hate crime, the school will consider whether the police should be contacted.
- As part of the school's ongoing commitment to the prevention of cyberbullying, regular education and discussion about e-safety will take place as part of computing and PSHE.

➔ 10. Training

At IncludEd Learning we recognise that early intervention can protect students who may be at risk of cyber bullying or negative social media behaviour. As such, teachers will receive training in identifying potentially at-risk students.

- Teachers and support staff will receive training on the Social Media Policy as part of their new starter induction.

- Teachers and support staff will receive training at least annually as part of their development.

- Students will be educated about e-safety and appropriate social media use on a termly basis through a variety of mediums, including: mentoring, PSHE lessons and cross-curricular links.

- Students will be provided with material to reinforce their knowledge.

- Information on e-safety and social media awareness is available on the school's website.

- Training and information for all students, staff and parents will be refreshed in light of any significant incidents or changes.

Monitoring and review

This policy will be reviewed on an annual basis by the Head of Centre, in conjunction with the DSL.

The next scheduled review date for this policy is November 2025.

Any changes made to this policy will be communicated to all staff, students and parents.

APPENDIX A : Blocked Content Access Request Form

Requester	
Staff name:	
Date:	
Full URL:	
Site content:	
Reasons for access:	
Identified risks and control measures:	
Authoriser	
Approved?	✔ / X
Reasons:	
Staff name:	
Date:	
Signature:	

APPENDIX B : Inappropriate Content Report Form

Staff name (submitting report):	
Name of individual accessing inappropriate content (if known):	
Date:	
Full URL(s):	
Nature of inappropriate content:	
To be completed by e-safety officer	
Action taken:	
Staff name:	
Date:	
Signature:	