Ocker Hill Academy

Social Media Policy

To be reviewed in line with Ocker Hill Academy Policy Guidelines

Contents:

Statement of intent

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

We are committed to:

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

1. Legal framework

1.1. 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

1.2. This policy will be implemented in accordance with the following Academy policies and documents:

- Parent and Visitor Conduct Policy
- Staff, Governor and Visitor Acceptable Use Agreement
- e-Safety Policy
- e-safety Leaflet for Pupils
- Data and E-Security Breach Prevention and Management Plan
- Data Protection Policy
- Pupil Code of Conduct
- Complaints Policy
- Anti-Bullying Policy
- Allegations Against Staff Policy
- Photography and Videos Policy

2. Roles and responsibilities

2.1. The Principal is responsible for:

- The overall implementation of this policy and ensuring that all staff, parents and pupils 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 governing board, handling complaints regarding this policy and its provisions in line with the Academy'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 the e-Safety Officer and Data Protection Officer (DPO) to ensure appropriate security measures are implemented and compliance with the GDPR.

2.2. Staff members are responsible for:

- Adhering to the principles outlined in this policy and the Technology Acceptable Use Agreement – Staff.
- Ensuring pupils 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, pupils or parents to the Principal immediately.
- Attending any training on social media use offered by the Academy.

2.3. Parents are responsible for:

- Adhering to the principles outlined in this policy and the Code of Conduct for Parents.
- 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 Ocker Hill Academy wherever possible.

2.4. Pupils are responsible for:

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

3. Definitions

3.1. For the purpose of this policy, Ocker Hill Academy 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
- Media-sharing devices, such as YouTube
- 'Micro-blogging' applications, such as Twitter
- On-line gaming, such as x-box live

3.2. 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.

3.3. For the purpose of this policy, "members of the Academy community" are defined as any teacher, member of support staff, pupil, parent of a pupil, governor or ex-pupil.

4. Data protection principles

4.1. The Academy will obtain consent from pupils and parents at the beginning of each academic year using the Images and Videos Parental Consent Form, which will confirm whether or not consent is given for posting images and videos of a pupil on social media platforms. The consent will be valid for the entire academic year.

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

4.3. For the purpose of section 4.1, Ocker Hill Academy will obtain consent from whoever holds parental responsibility for the child.

4.4. Parents are able to withdraw or amend their consent at any time. To do so, parents must inform the Academy in writing.

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

4.6. Where parents 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' requirements following this.

4.7. In line with section 4.5, wherever it is reasonably practicable to do so, the Academy will take measures to remove any posts before consent was withdrawn or amended, such as removing an image from a social media site.

4.8. The Academy will only post images and videos of pupils for whom consent has been received.

4.9. Only Academy-owned devices will be used to take images and videos of the Academy community, which have been pre-approved by the e-Safety Officer for use.

4.10. When posting images and videos of pupils, the Academy will apply data minimisation techniques, such as pseudonymisation (blurring a photograph), to reduce the risk of a pupil being identified.

4.11. The Academy will not post pupils' personal details on social media platforms.

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

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

4.14. When posting on social media, Ocker Hill Academy will use group or class images or videos with general labels, e.g. 'sports day'.

4.15. Before posting on social media, staff will:

- Refer to the consent record log to ensure consent has been received for that pupil and for the exact processing activities required.
- Ensure that there is no additional identifying information relating to a pupil.

4.16. Any breaches of the data protection principles will be handled in accordance with the Academy's Data and E-Security Breach Prevention and Management Plan.

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

5. Social media use – staff

Academy accounts

5.1. Academy social media passwords are kept securely in the Academy office – these are not shared with any unauthorised persons, including pupils, unless otherwise permitted by the Principal.

5.2. Staff will ensure any posts are positive in nature and relevant to pupils, the work of staff, the Academy or any achievements.

5.3. Staff will ensure that a member of the SLT has checked the content before anything is posted on social media.

5.4. Staff will adhere to the data protection principles outlined in section 4 of this policy at all times.

5.5. Staff will not post any content online which is damaging to the Academy or any of its staff or pupils.

5.6. If inappropriate content is accessed online, a report form will be completed and passed on to the e-Safety Officer. The e-Safety Officer retains the right to monitor staff members' internet usage in line with the Data and E-Security Breach Prevention and Management Plan.

Personal accounts

5.7. Staff members will not access social media platforms during lesson times.

5.8. Staff members will not use any Academy-owned mobile devices to access personal accounts, unless it is beneficial to the material being taught – prior permission will be sought from the principal.

5.9. Staff members are permitted to use social media during break times.

5.10. Staff are not permitted to use the academy's Wi Fi network to access personal accounts, unless otherwise permitted by the Principal, and once the e-safety officer has ensured the necessary network security controls are applied.

5.11. Staff will avoid using social media in front of pupils.

5.12. Staff will not "friend" or otherwise contact pupils or parents through their personal social media accounts.

5.13. If pupils or parents attempt to "friend" a staff member they will report this to the Principal.

5.14. Staff members will not provide their home address, phone number, mobile number, social networking details or email addresses to pupils or parents – any contact with pupils or parents will be done through authorised Academy contact channels.

5.15. Staff members will ensure the necessary privacy controls are applied to personal accounts.

5.16. Staff members will avoid identifying themselves as an employee of Ocker Hill Academy on their personal social media accounts.

5.17. No staff member will post any content online that is damaging to the Academy or any of its staff or pupils.

5.18. 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 Ocker Hill Academy.

5.19. Staff members will not post any information which could identify a pupil, class or the Academy – this includes any images, videos and personal information.

5.20. Staff will not take any posts, images or videos from social media that belong to the academy for their own personal use.

5.21. Staff members will not post anonymously or under an alias to evade the guidance given in this policy.

5.22. 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.

5.23. Members of staff will be aware that if their out-of-work activity brings the Academy into disrepute, disciplinary action will be taken.

5.24. Members of staff will regularly check their online presence for negative content via search engines.

5.25. Attempts to bully, coerce or manipulate members of the Academy community via social media by members of staff will be dealt with as a disciplinary matter.

5.26. Members of staff will not leave a computer or other device logged in when away from their desk or save passwords.

5.27. Staff members will use their Academy email address for Academy business and personal email address for their private correspondence; the two should not be mixed.

6. Social media use – pupils and parents

6.1. Pupils will not access social media during lesson time, unless it is part of a curriculum activity.

6.2. Pupils and parents will not attempt to "friend" or otherwise contact members of staff through their personal social media accounts. Pupils and parents are only permitted to be affiliates of Academy social media accounts.

6.3. Where a pupil or parent attempts to "friend" a staff member on their personal account, it will be reported to the Principal.

6.4. Pupils and parents will not post anonymously or under an alias to evade the guidance given in this policy.

6.5. Pupils and parents will not post any content online which is damaging to Ocker Hill Academy or any of its staff or pupils.

6.6. Pupils are instructed not to sign up to any social media sites that have an age restriction above the pupil's age.

6.7. If inappropriate content is accessed online on Academy premises, it will be reported to a teacher.

6.8. Pupils are not permitted to use the Academy's Wi Fi network to access any social media platforms unless prior permission has been sought from the Principal, and the e-Safety Officer has ensured appropriate network security measures are applied.

6.9. Parents are not permitted to use the Academy's Wi Fi network to access any social media platforms on personal devices. Social media access on an Academy-owned device may be permitted in line with 6.8.

6.10. Breaches of this policy will be taken seriously, and in the event of illegal, defamatory or discriminatory content could lead to prosecution, or exclusion.

7. Blocked content

7.1. In accordance with Ocker Hill Academy's Data and E-Security Breach Prevention and Management Plan, the e-Safety Officer installs firewalls on the Academy's network to prevent access to certain websites. The following social media websites are not accessible on the Academy's network:

- Facebook

- Instagram

7.2. Attempts made to circumvent the network's firewalls will result in a ban from using Academy computing equipment, other than with close supervision.

7.3. Inappropriate content accessed on the Academy's computers will be reported to the e-Safety Officer so that the site can be blocked.

7.4. The e-Safety Officer retains the right to monitor staff and pupil access to websites when using the Academy's network and on Academy-owned devices.

7.5. Requests may be made to access erroneously blocked content by submitting a blocked content access form to the e-Safety Officer, which will be approved by the Principal.

8. Cyber bullying

8.1. Cyber bullying incidents are taken seriously at Ocker Hill Academy. Any reports of cyber bullying on social media platforms by pupils will be handled in accordance with the Anti-Bullying Policy.

8.2. Allegations of cyber bullying from staff members will be handled in accordance with the Allegations of Abuse against Staff Policy.

8.3. Staff members will not respond or retaliate to cyber bullying incidents. Incidents will be reported as inappropriate, and support will be sought from the principal.

8.4. Evidence from the incident will be saved, including screen prints of messages or web pages, and the time and date of the incident.

8.5. Where the perpetrator is a current pupil or colleague, most incidents can be handled through the Academy's own disciplinary procedures.

8.6. 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.

8.7. If the perpetrator refuses to comply, it is up to the Academy 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.

8.8. If the material is threatening, abusive, sexist, of a sexual nature or constitutes a hate crime, Ocker Hill Academy will consider whether the police should be contacted.

8.9. As part of the Academy's ongoing commitment to the prevention of cyber bullying, regular education and discussion about e-safety will take place as part of computing and PSHE.

9. Training

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

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

9.3. Teachers and support staff will receive annual training as part of their development.

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

9.5. Pupils will be provided with material to reinforce their knowledge, such as our E-Safety Leaflet for Pupils.

9.6. Parents will be invited to e-safety and social media training on an annual basis and provided with relevant resources, such as our Code of Conduct for Parents.

9.7. Training for all pupils, staff and parents will be refreshed in light of any significant incidents or changes.

10. Monitoring and review

10.1. This policy will be reviewed in line with Ocker Hill Academy Policy Guidelines

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:	

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:	