Ormiston Academies Trust

Sandymoor Ormiston Academy Social Media Policy

Policy version control

Policy type	Strongly recommended
Author: In consultation with:	Kerry Barry Alexandra Coughlan
Approved by	Carmel Brown, March 2022
Release date	March 2022
Next release date	March 2024
Description of changes	Amended section 4 as it's not talking about data protection principles, it's specifically talking about consent, and then a line in section 5 to reflect that. Also updated GDPR to say UK GDPR.

Contents

Statement of intent

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

We are committed to:

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

Signed by:

_____	Principal	Date:	24.03.22
_____	Chair of Governors	Date:	24.03.22

1.Legal framework

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

- The UK General Data Protection Regulation (UK 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 school policies and documents:

- E-Safety and E-Security Policy
- Data Protection and Freedom of Information Policy
- Child Protection and Safeguarding Policy
- Staff guidelines for social media channels
- Staff Disciplinary Policy
- Complaints Policy
- Anti-Bullying Policy
- Allegations of Abuse Against Staff Policy
- Technology Acceptable Use Policy (AUP) Academy Workforce Agreement
- Photography and Video Policy

2.Roles and responsibilities

2.1. The principal is responsible for:

- The overall implementation of this policy and ensuring that all staff, parents/carers 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 school's complaints procedures.
- 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 Data Protection Lead (DPL) to ensure appropriate security measures are implemented and compliance with the UK GDPR.

2.2. Staff members are responsible for:

- Adhering to the principles outlined in this policy.
- Educating pupils about the principles outlined in this policy and that it is implemented fairly and consistently.
- Reporting any social media misuse by staff, pupils or parents/carers to the principal immediately.

- Attending any training on social media use offered by the school or Ormiston Academies Trust (the Trust).

2.3. Parents/carers are responsible for:

- 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/workshops held by the school wherever possible.

2.4. Pupils are responsible for:

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

3. Definitions

3.1. For the purpose of this policy, the school defines "social media" as any online channel/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
- Collaborative spaces, such as Facebook
- Media-sharing devices, such as YouTube
- 'Micro-blogging' applications, such as Twitter
- Photograph and video sharing spaces, such Instagram and TikTok

3.2. For the purpose of this policy, "cyber bullying" is defined as any social media or communication technology intentionally used to bully (use of force, coercion, or threat, to abuse, aggressively dominate or intimidate) 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 school community"** are defined as any teacher, member of support staff, pupil, parent/carer of a pupil or governor.

4. Consent to use of images

4.1. The school will obtain consent from pupils and parents/carers in line with the Photography and Video Policy and 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 duration of a pupil's time at the school and for a period of two years after they have left the school, unless the pupil's circumstances change in any way (eg. if consent is withdrawn).

4.2. A record of consent is maintained throughout the academic year, which details the pupils for whom consent has been provided. The Schools' Designated Safeguarding Lead (DSL) and Data Protection Lead (DPL) are responsible for ensuring this consent record remains up-to-date.

4.3. For the purpose of section 4.1, where a pupil is assessed by the school to have the competence to understand what they are consenting to, the school will obtain consent directly from that pupil; otherwise, consent is obtained from whoever holds parental responsibility for the child.

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

4.5. Consent can be provided for certain principles only, for example only images and videos of a pupil are permitted to be posted. This will be made explicitly clear on the consent from provided.

4.6. Where parents/carers or pupils would like to withdraw/amend consent this will affect all future processing. However, if parents/carers or pupils would like to remove images and videos prior to consent being withdrawn/amended they will need to make this clear.

4.7. Only school-owned devices or agreed equipment will be used to take images and videos of the school community, which have been pre-approved by the principal for use.

4.8. The school will not post pupils' personal details (which include identifiable references about home address and information about family members) on social media platforms.

4.9. A pupil's full name will never be used alongside any videos or images in which they are present, unless permission/consent has been given.

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

4.11. When posting on social media, the school will use group or class photographs or videos with general labels, eg. 'sports day'.

4.12. 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 any additional identifying information relating to a pupil is carefully considered before posting.

4.13. Any breaches of the data protection principles will be handled in accordance with the school's Data Protection and Freedom of Information Policy.

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

5.Social media use – staff

5.1. School accounts

5.1.1. School social media passwords are kept in the school office – these are not shared with any unauthorised persons, including pupils, unless otherwise permitted by the principal.

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

5.1.3. Staff will ensure the principal, member of the senior leadership team (SLT) or the comms lead has sight/checked the content before anything is posted on social media.

5.1.4. If staff wish for reminders to be posted for parents/carers, eg. returning slips for a school trip, staff will seek permission from the principal, member of SLT, comms lead or student services team before anything is posted.

5.1.5. At all times staff will ensure images of pupils are only used in line with consent obtained, as outlined in section 4 of this policy.

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

5.1.7. If inappropriate content is accessed online, a report form (see annexe 1) will be completed and passed on to the principal. The principal retains the right to monitor staff members' internet usage in line with the Data Protection and Freedom of Information Policy.

5.2. Personal accounts

5.3. Staff members will not access social media platforms during lesson times unless approval is sought via the principal.

5.4. 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 principal.

5.5. If permission has been given, staff members are permitted to use social media during break times.

5.6. Staff are not permitted to use the school's WiFi network to access personal accounts, unless otherwise permitted by the principal, and once the IT team has ensured the necessary network security controls are applied.

5.7. Staff will avoid using social media in front of pupils within the classroom to model good practice and behaviour, unless it is beneficial to the material being taught.

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

5.9. If pupils or parents/carers attempt to "friend" a staff member they will report this to the principal.

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

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

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

5.13. 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 school.

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

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

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

5.17. 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.

5.18. Members of staff will be aware that if their out-of-work activity (which may include political, sexual or alcohol) brings the school into disrepute, disciplinary action will be taken.

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

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

5.21. 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.

6.Social media use – pupils and parents/carers

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

6.2. Pupils and parents/carers will not attempt to “friend” or otherwise contact members of staff through their personal social media accounts.

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

6.4. Staff members will not accept pupils or parents/carer as “friends” on social media accounts unless the Principal agrees to it because the pupil or parent/carer is known by the staff member outside of their school role (i.e. family or close friend).

6.5. Pupils and parents/carers are encouraged not to post anonymously or under an alias to evade the guidance given in this policy.

6.6. Pupils and parents/carers are encouraged not to post any content online which is damaging to the school or any of its staff or pupils.

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

6.8. If inappropriate content is accessed online on school premises it will be picked up my IT systems and will be reported to a member of staff.

6.9. 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 the school's Data Protection and Freedom of Information Policy. Firewalls are installed on the school's network to prevent access to certain websites that may be considered as inappropriate. The following social media websites are not accessible on the school's network, unless permission is given:

- Twitter
- Facebook
- Instagram
- TikTok

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

7.3. Inappropriate content accessed on the school's computers is monitored via IT systems and will be reported to the IT team so that the site can be blocked.

7.4. The IT team and principal retains the right to monitor staff and pupil access to websites when using the school's network and on school-owned devices.

7.5. Requests may be made to access erroneously blocked content by submitting a blocked content access form (see annexe 2) to the IT team, which will be approved by the principal.

8.Cyber bullying

8.1. Cyber bullying incidents are taken seriously at school. 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 school'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 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.

8.8. 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.

8.9. As part of the school'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 school, 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 termly and ongoing training as part of their development.

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

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

10. Monitoring and review

10.1. This policy will be reviewed every two years by the principal, in conjunction with the OAT, Safeguarding, IT team and DPO.

10.2. The next scheduled review date for this policy is February 2024.

10.3. Any changes made to this policy will be communicated to all staff, pupils and parents/carers.

Annexe 1

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:	

Annexe 2

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 a member of the IT team	
Action taken:	
Staff name:	
Date:	
Signature:	