



# Social Media Policy

<b>Policy Code:</b>	IT4b
<b>Policy Start Date:</b>	September 2021
<b>Policy Review Date:</b>	September 2022

## **Statement of Intent**

CIT Academies 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:

- Encouraging the responsible use of social media by all staff, parents and pupils in support of the school's mission, values and objectives.
- Protecting our pupils 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.

## **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 Regulations (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 Trust policies and documents:

- Acceptable Use of the Internet Policy
- Allegations of Abuse against Staff Policy
- Communications Policy
- Child Protection & Safeguarding Policy
- Data Protection Policy
- Staff Code of Conduct
- Complaints Policy

## **2. Roles and responsibilities**

2.1 The Head Teacher 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 Trust Board, ELT and Local School Board, handling complaints regarding this policy and its provisions in line with the CIT Complaints 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 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 Acceptable Use of the Internet Policy.
- Ensuring pupils follow 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 Head Teacher immediately.
- Attending any training on social media use offered by the school.

2.3 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.

### 3. **Definitions**

3.1 For the purpose of this policy, the Trust 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
- Media-sharing devices, such as YouTube
- ‘Micro-blogging’ applications, such as Twitter

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 school community” are defined as any Member, Trustee, senior leader, teacher, member of support staff, pupil, parent or carer of a pupil, Governor or ex-pupil.

### 4. **Data Protection principles**

4.1 The school will obtain consent from pupils and parents and carers at the beginning of their enrolment at the school using the parental consent form, which will confirm whether or not consent is given for posting images and videos of a pupil on the school website, social media pages, and/or in the media. The consent will be valid for the pupil’s time at the school.

4.2 For the purpose of section 4.1, where a pupil is aged 18 and over and 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.

- 4.3 Parents and pupils are able to withdraw or amend their consent at any time. To do so, parents and pupils must inform the school in writing.
- 4.4 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 form provided.
- 4.5 Where parents or pupils withdraw or amend their consent, it will not affect the processing of any images or videos prior to when consent was withdrawn or amended, unless specifically requested. Processing will cease in line with parents' and pupils' requirements following this.
- 4.6 In line with section 4.5, 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.
- 4.7 The school will only post images and videos of pupils for whom consent has been received.
- 4.8 Only school-owned devices may be used by school staff to take images and videos of the school community, which have been pre-approved by the DPO for use.
- 4.9 The school will not post pupils' personal details on social media platforms.
- 4.10 Pupils' full names will not be used alongside any videos or images in which they are present, unless a parent/carer has specified to do so.
- 4.11 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.

## **5. Social media use – staff**

### **School accounts**

- 5.1 School social media passwords are not shared with any unauthorised persons, including pupils, unless otherwise permitted by the Head Teacher.
- 5.2 Staff will ensure any posts are positive in nature and relevant to pupils, the work of staff, the school or any achievements.
- 5.3 If staff wish for reminders to be posted for parents, e.g. returning slips for a school trip, staff will seek permission from the Head Teacher before anything is posted.
- 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 school or any of its staff or pupils.

- 5.6 If inappropriate content is accessed online, this must be reported to the DPO immediately. The DPO retains the right to monitor staff members' Internet usage in line with the Data Protection Policy.

### **Personal accounts**

- 5.7 Staff members will not access social media platforms during lesson times, unless it forms part of a planned lesson.
- 5.8 Staff members are permitted to use social media during break times, away from pupils.
- 5.9 Staff will avoid using social media in front of pupils.
- 5.10 Staff will not "friend" or otherwise contact pupils or parents through their personal social media accounts unless prior approval is sort from the Head Teacher. An exception is in the case of blogs or social media pages set up specifically for the purpose of teaching and learning.
- 5.11 Staff members will not provide their home address, personal phone number, mobile number, social networking details or personal email addresses to pupils or parents – any contact with pupils or parents will be done through authorised school contact channels.
- 5.12 Staff members will ensure the necessary privacy controls are applied to personal accounts.
- 5.13 No staff member will post any content online that is damaging to CIT Academies or any of its staff or pupils.
- 5.14 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 the school.
- 5.15 Staff members will not post any information which could identify a pupil, class or the school – this includes any images, videos and personal information.
- 5.16 Staff will not take any posts, images or videos from social media that belong to the school for their own personal use.
- 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 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 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.
- 5.21 Members of staff will not leave a computer or other device logged in when away from their desk or save passwords.

5.22 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**

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

6.2 Pupils and parents should 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 school 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 Head Teacher.

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

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

6.6 Pupils are not permitted to use the school’s Wi-Fi network to access any social media platforms unless prior permission has been sought from the Head Teacher, and the DPO has ensured appropriate network security measures are applied.

6.7 Parents are not permitted to use the school’s Wi-Fi network to access any social media platforms on personal devices. Social media access on school-owned devices may be permitted in line with 6.8.

6.8 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 Policy, the DPO 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

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 will be reported to the DPO so that the site can be blocked.

7.4 The DPO retains the right to monitor staff and pupil access to websites when using the school’s network and on school-owned devices.

## **8. Cyber bullying**

8.1 Cyber bullying incidents are taken seriously across CIT Academies 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 Head Teacher.
- 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 Across CIT Academies 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 are made aware of the Social Media Policy as part of their new starter induction.
- 9.3 Teachers and support staff will receive ongoing 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 e-safety leaflets.
- 9.6 Parents will be invited to e-safety and social media training when provided.
- 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 on an annual basis by the Head of Communications, in conjunction with the DPO.

10.2 The next scheduled review date for this policy is September 2022.

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