Social Media Policy

Audience:	REAch2 Staff Volunteers Local Governing Bodies Trustees
Ratified:	NJCC - October 2024 Executive Team – November 2024
Policy owner:	Sue Northend, Director of People
Review:	Every 3 years

At REAch2, our actions and our intentions as school leaders are guided by our Touchstones.

Policy Overview

Statement of Intent
REAch2 understands that social media is integral to how we communicate with each other today and recognises the benefits of social media to enable networking, to sharing learning and best practice, to promoting our schools, to attracting talented staff and to building relationships with parents and within the local community.

We have a responsibility to safeguard our children against potential dangers when accessing the internet at school, and to educate our staff and children about how to protect themselves online when not in school. Staff members must therefore be conscious, at all times, when they are using social media, of the need to keep their personal and professional lives separate and to be mindful of their responsibility to protect the reputation of their school and of the Trust.

This policy sets out the principles that all employees and representatives of REAch2 are expected to follow when using social media.

We are committed to:

- Encouraging the responsible use of social media by all staff, volunteers, parents and children.
- Protecting our children from the dangers of social media.
- Preventing damage to the reputation of the Trust through irresponsible use of social media.
- Protecting our staff from cyberbullying.
- Taking a firm stance when social media is used to promote discrimination or violent harm to others.

Legal Framework
This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- Department for Education (DfE) (2023) 'Data protection in schools'
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Computer Misuse Act 1990, amended by the Police and Justice Act 2006
- Freedom of Information Act 2000
- Safeguarding Vulnerable Groups Act 2006
- Equality Act 2010

- DfE 'Keeping Children Safe in Education'

Roles and Responsibilities

The Headteacher / Line Manager is responsible for:

- The implementation of this policy across the school / direct reports.
- Ensuring that all staff and volunteers are aware of their responsibilities in relation to social media use.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction.
- Promoting safe working practices and standards with regards to the use of social media.
- Establishing clear expectations with regards to the use of social media.
- Implementing the disciplinary procedure and appropriate sanctions where there is a breach of this policy.

The DSL is responsible for:

- The school's approach to online safety.
- Dealing with concerns about social media use in school that are safeguarding concerns.

Staff members will be responsible for:

- Adhering to the principles outlined in this policy.
- Reporting any social media misuse immediately.
- Attending any training on social media use.

The Trust will support schools in:

- Providing support in the development and implementation of social media accounts.
- Implementing appropriate security measures.
- Ensuring that the Trust's filtering and monitoring systems are up to date.

Policy In Detail

School Social Media Accounts

A school-based social media account will be entirely separate from any personal accounts held by staff members and will be linked to an official school email account. Staff members must not use work-related email addresses to set up a personal social media account.

The only exception to this is Facebook which requires a personal Facebook account to be linked to a Facebook Group/Page to update and administer content. This will only be permitted through 'Facebook Business Manager' which allows the Trust to control access permissions for individuals within the Trust and invites must be sent to the official school email account where it can then be linked a personal Facebook account. You must seek guidance from the Brand, Marketing and Communications team to facilitate this.

The Headteacher will be responsible for authorising members of staff and any other individual to have administration access to school social media accounts and posting on the school's accounts.

Passwords for the school's social media accounts will be stored securely and shared with the Marketing to ensure that emergency support can be provided in the absence of the nominated school administrator.

Passwords are only to be shared with people authorised by the Headteacher.

Posts made to school social media accounts will not breach copyright, data protection or freedom of information legislation.

School Staff Conduct

Any information obtained, or accessed, while undertaking work-related duties must not be disclosed via social media, nor without the express authorisation from a Headteacher, Head of Service or Director. Staff will only post content that meets the school's social media objectives, for example:

- Useful information about the school
- Reminders about upcoming events
- Good news regarding the school's performance, attainment or reputation
- Good news regarding the achievements of staff and children
- Information that parents should be aware of, e.g. school closure

Staff will ensure that any posts meet the following criteria:

- The post does not risk bringing the school into disrepute.
- The post does not include any personal views.
- The post uses appropriate and school-friendly language.

- The post is sensitive towards those who will read it.
- The post does not contain any wording or content that could be construed as offensive.
- The post does not take a side in any political debate or express political opinions.
- The post does not contain any illegal or unlawful content.

Staff use of personal social media accounts

Staff should be mindful of professional standards associated with their job role, irrespective of whether their actions are online, offline, before, during or after working hours. It is important that staff protect the reputation of the school / REAch2 by ensuring they use personal social media accounts in a respectful manner.

Anyone working on behalf of the Trust is legally bound by a duty of confidence to protect the data to which they have access to during the course of their work.

Staff are required to adhere to the following when using personal social media accounts:

- To ensure the necessary privacy controls are applied to personal accounts.
- To ensure that views posted on personal accounts are personal and are not those of the school or REAch2.
- To refrain from sharing confidential / privileged information, discussing incidents, operational or employment matters or making critical / negative comments about the school, about REAch2 or about pupils / parents or colleagues.
- Not to access personal social media during working hours apart from at break or lunch times.
- Not to use any school-owned mobile devices to access personal accounts.
- Not to 'friend', 'follow' or otherwise contact children through their personal social media accounts. If a child attempts to 'friend' or 'follow' a staff member, this should be reported to the DSL, Headteacher or line manager.
- Not to share discriminatory, defamatory, illegal, or violent content.
- Not to post any content online that is damaging to a school, REAch2, its staff or children.
- Not to post any information which could identify a child including images, videos and personal information.
- Not to post anonymously or under an alias to evade the guidance in this policy.
- Not to browse, create, transmit, display, publish, comment on or forward any material or images which are illegal, could offend or harass, or anything that could bring a staff member's professional role or the Trust's reputation into disrepute.
- Not to post images or videos of colleagues without permission.

Gross Misconduct

Breaches of this policy will be taken seriously and may lead to disciplinary action. Illegal, defamatory or discriminatory content may lead to prosecution and disciplinary action up to and including dismissal.

The following are likely to be considered as gross misconduct and, subject to a reasonable and fair investigation process, may result in dismissal without notice (summary dismissal):

- Wilful non-compliance with confidentiality and data protection principles, for example deliberate or reckless disclosure(s) of personal data held by the Trust or its academies without authorisation
- Wholly inappropriate use of any Trust device, or software, provided by the Trust for work-related purposes, including deliberately accessing internet sites containing pornographic, offensive or obscene material
- Unlawful discrimination, bullying or harassment or serious mistreatment of another person
- Abusive or threatening conduct towards others including victimisation, derogatory comments, demeaning jokes, or malicious rumours about an individual that has the effect of causing offense, distress, embarrassment, humiliation or intimidation.

Freedom of Expression

The Trust recognises that freedom of expression is a fundamental right and staff have the right to express their religious, political and philosophical beliefs in the workplace.

Freedom of expression will not be accepted as justification for making statements or comments that discriminate against, or harass, or incite violence or hatred against other people or specific groups particularly by reference to their characteristics.

Safeguarding

SENSO is REAch2's online monitoring system. It is installed on all compatible Trust devices. SENSO captures a screenshot of the device screen when any language has been used that is considered a concern or risk, based on an extensive library of words and phrases. In line with statutory guidance and the Trust's Safeguarding Policy, Headteachers and line managers are responsible for responding to any risks arising from alerts reported by SENSO for staff devices.

Concerns about a staff member's online behaviour will be reported to the Headteacher, or line manager, who will decide on the best course of action in line with the relevant policy.

Where there is a concern that illegal activity has taken place, the police will be contacted.

Blocked content

The Trust's IT Team install firewalls on the network to prevent access to certain websites. Social media websites are not accessible on REAch's network, except for specified staff devices approved by the Headteacher, by the Marketing Team and managed by the Trust's IT team.

The Trust's IT Team retains the right to monitor access to websites when using the Trust's network and on Trust-owned devices. Attempts made to circumvent the network's firewalls will result in a ban from using Trust devices.

Requests may be made to access blocked content by submitting a request to IT@reach2.org or submitting a ticket via the REAch2 Help icon.

Cyberbullying
Cyberbullying will not be tolerated under any circumstances. Incidents of cyberbullying will be dealt with quickly and effectively wherever they occur. Allegations of cyberbullying from staff members will be handled in accordance with the Dignity at Work Policy.

Policy Review

This policy will be reviewed every 3 years or sooner, taking into account any legislative changes or following an online safety incident.
Any changes made to this policy will be communicated to all relevant stakeholders.