Social Media and Social Networking Policy

Approved by: Raúl Fernández Pascual, Principal, Colegio CEDES	**Last reviewed on:** June 2026
Next review due by: June 2027	

1. Purpose

- This policy aims to:
- set guidelines and rules for the use of the **Colegio CEDES** 's social media channels;
- establish clear expectations for the way members of the Colegio CEDES community engage with each other online;
- support the school's safeguarding, online safety and data protection processes.

2. Scope

For the purposes of this document, social media and social networking are considered to include all technologies that allow individuals to communicate and share information, including photos and video. This includes group messaging services (such as WhatsApp) and online gaming platforms (such as Minecraft).

This policy applies to the use of social media for both business and personal purposes, whether during school/working hours or outside these times. It applies regardless of whether the social media is accessed using:

- school IT equipment, facilities and networks;
- devices or equipment belonging to members of staff and students;
- any other IT/internet-enabled devices, equipment and networks.

All members of the school community should bear in mind that information they share through social networking applications, even if they are on private spaces, may be subject to copyright, safeguarding and data protection or other legislation.

All members of the **Colegio CEDES** community must operate in line with the school's policies, and all staff, academic or administrative, are required to read, understand and comply with this policy.

2.1 Legislation and Guidance

While breaches of this policy will be considered a serious conduct matter which may lead to disciplinary action being taken under the school's Behaviour and Disciplinary Policies, inappropriate use of social media or social networking may also result in civil or criminal liability under laws relating to:

- **Confidentiality and privacy**, notably Organic Law 3/2018 on Personal Data Protection and Guarantee of Digital Rights (LOPDGDD) and Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR).
- **Equality and non-discrimination**, including the Spanish Constitution, Organic Law 3/2007 for the Effective Equality of Women and Men, and Law 15/2022 on Equal Treatment and Non-Discrimination.
- **Libel, defamation, harassment and breach of copyright**, including the Spanish Criminal Code (Organic Law 10/1995), Organic Law 1/1982 on the Civil Protection of the Right to Honour, Personal and Family Privacy and Personal Image, and Royal Legislative Decree 1/1996 approving the consolidated text of the Intellectual Property Law.

2.2 Personal Use of Social Media by Staff

The school expects all staff, including members of the Board and volunteers, to consider the safety and wellbeing of students, their professional responsibilities and the potential reputational and financial risks to the school when using social media, including when doing so in a personal capacity.

Staff must maintain a clear separation between their personal and professional online presence. Personal social media accounts must be set to private, in accordance with Ariston Education safeguarding standards, and staff are responsible for regularly checking and maintaining appropriate privacy and security settings.

Staff members must report any safeguarding concerns they become aware of through social media or other online platforms.

When using social media, staff must not:

- use personal accounts to conduct school business;
- accept or send ‘friend’ or ‘follow’ requests to current students, or communicate with them through personal social media accounts;
- reference or share confidential or personal information about individual students, colleagues or parents/carers;
- post comments about the school, students, colleagues or parents/carers that are inappropriate, disrespectful or could bring the school into disrepute;
- post or share images, videos or recordings of students through personal accounts;
- express personal views or opinions in a way that could reasonably be interpreted as representing the school;
- link personal social media profiles to their school email account;
- use personal social media during timetabled teaching time, except where its use has been specifically authorised for a professional or educational purpose;
- share personal information with students, such as personal telephone numbers, home addresses or other private contact details.

All communications between staff and students or parents/carers must take place through official school communication channels.

Any communication received from a current student, unless they are a family member, through a member of staff’s personal social media account must be reported to the Designated Safeguarding Lead (DSL) immediately. Staff must not continue the communication through the personal account.

Staff should not maintain contact with former students through personal social media accounts where this could compromise professional boundaries or give rise to a safeguarding concern. Where ongoing communication is required for a legitimate professional purpose, it must take place through official school channels.

Any concerns regarding a member of staff’s personal use of social media will be managed in accordance with the Staff Code of Conduct and the school’s safeguarding procedures.

2.3 Personal Use of Social Media by Students

The school encourages students to:

- be respectful towards the school, members of staff, other students and parents/ carers at all times;
- direct any concerns or complaints through the school’s official channels, so they can be dealt with in line with the school’s behaviour or complaints procedures.
- Students should not use social media to:
- complain about the school or bring the school into disrepute;
- complain about individual members of staff or other students;
- make inappropriate comments about members of staff, other students or parents/carers;
- post images and/or audio, including those generated by AI, of staff or other students without their permission.
- Any concerns about a student’s social media use will be dealt with in line with the school’s Behaviour and Online Safety policies.

2.4 Personal Use of Social Media by Parents/Carers

The school expects parents/carers to help us model safe, responsible and appropriate social media use for our students.

When communicating with the school via official communication channels, or using private/independent channels to talk about the school, parents and carers should:

- be respectful towards, and about, members of staff and the school at all times;
- be respectful of, and about, other parents/carers and other students and children;
- direct any concerns or complaints through the school's official channels, so they can be dealt with in line with the school's Concerns and Complaints Policy.

Parents/carers should not use social media to:

- complain about the school;
- complain about individual members of staff, students or other parents/carers;
- make inappropriate comments about members of staff, students or other parents/carers;
- draw attention to, or discuss, behaviour incidents;
- post images of children other than their own.

Every reasonable effort will be taken to politely address concerns or behaviour of individual users, in line with the school's Concerns and Complaints Policy. However, if users are repeatedly abusive or post inappropriate content that affects the school's community and policies, the school will take every measure to ensure they are blocked by the designated moderator.

WhatsApp and similar messaging platforms can provide quick and effective communication among groups, such as parents in a class. Parents/carers should follow the same social media guidelines (above) when using WhatsApp groups.

3. Monitoring of and Access to Social Media

Colegio CEDES reserves the right to monitor, intercept and review any and all activities using the school's IT resources and communications systems, including social media postings and messaging. This includes ascertaining and demonstrating that expected standards are being met by those using the systems, and the detection and investigation of improper or unauthorised use of the systems (especially where this is necessary to prevent or detect criminal activity).

By using the school's IT resources and facilities, all members of the Colegio CEDES community and other visitors give the school consent to monitor their activities. All should be aware that their use of social media and any information published by them may be monitored and reviewed.

Colegio CEDES reserves the right to disable social media traffic on key networks within the school, such as wi-fi and wired networks used for teaching, where the use of social networking is not appropriate.

4. Reporting

Concerns about breaches of this policy should be sent to the Principal. Details of the investigation process and potential outcomes are set out in the Online Safety Policy.

5. Training and Awareness

All staff receive regular online safety training, which includes the use and risks of social media, as part of their CPD and mandatory training plan. New staff receive online safety training, which includes the use of social media, as part of their induction, completed within the first 3 weeks

To support students and parents, the school will raise awareness about the appropriate use and potential risks of social media, and provide regular information through:

- curriculum-linked activities
- communications (e.g. letters, newsletters, website, learning platform)
- parent sessions, workshops and events

- campaigns (e.g. Safer Internet Day)
- signposting to trusted resources (e.g. saferinternet.org.uk, childnet.com)
- providing information and resources to support online safety at home

6. Monitoring and Review

Working with the IT Manager and Designated Safeguarding Lead, the Principal will monitor the implementation of this policy, and ensure it is updated to reflect the needs and circumstances of the school and the social media channels and tools available to users.

This policy will be reviewed each year.

On behalf of the Board, the Regional Head of Schools is responsible for approving this policy.

7. Related Policies

This policy should be read in conjunction with the following documents:

- Safeguarding & Child Protection Policy
- Acceptable Use of IT, Online Safety and Mobile Phone policies
- Behaviour and Anti-Bullying policies
- Staff Behaviour/Code of Conduct
- Data Protection Policy
- Equality, Diversity and Inclusion Policy
- Child-on-Child Abuse Policy
- Low-Level Concerns Policy
- Allegations Against Staff Policy
- Whistleblowing Policy