

St Joseph's Catholic Primary School



Our Mission Statement

We grow together in God's Love as we Pray, Learn and Play

"Dyn ni'n tyfu gyda'n gilydd mewn cariad Duw wrth i ni weddio, dysgu a chwarae"

SOCIAL MEDIA POLICY

Article 16:

You have the right to have privacy

Social Media Policy for St. Joseph's RC Primary School

1. Introduction

Social media refers to a range of web-based applications and online platforms that allow people to create, communicate and exchange content. Social media is widely used through platforms such as Facebook, Instagram, YouTube, Snapchat, TikTok, LinkedIn and X, as well as blogs, email, texting and instant messaging.

- When used responsibly and appropriately, social media can offer education practitioners a number of benefits, including:
 - Building and maintaining professional relationships.
 - Accessing professional support networks and opportunities to discuss professional issues and share good practice.
 - Accessing professional learning opportunities and educational resources.
 - Supporting communication and engagement with the wider school community through approved school accounts.
- However, there are also a number of dangers and potential pitfalls associated with social media use. This policy provides clear guidance regarding the expectations of all staff at St Joseph's RC Primary School. It highlights how inappropriate use of social media and IT facilities may affect an individual's professional reputation, their relationship with the school community and, where appropriate, their employment.
- All staff who are registered with the Education Workforce Council (EWC) are subject to the **Code of Professional Conduct and Practice**. Staff must ensure that their online conduct is consistent with the professional standards expected of them.

This policy should therefore be read alongside the school's other relevant policies, including:

- Child Protection and Safeguarding Policy
- Online Safety Policy
- Data Protection and GDPR Policy
- Staff Code of Conduct
- Acceptable Use Agreements
- Disciplinary Policy and Procedures

2. Common Issues Facing Education Professionals

- The way staff use social media in their private lives is a matter for their own personal judgement. However, staff should exercise caution regarding the content they upload or share and consider whether it could compromise public confidence in themselves, their profession or the school.
- Social media can blur the boundaries between an individual's private and professional life. Staff should be aware that pupils, parents/carers, members of the public and prospective employers may be able to access information about them online.

- Staff should therefore consider carefully which social media platforms they use, what information they share and with whom they communicate.
- Staff should bear in mind that:
 - a) The professional standards expected of staff do not change because communication takes place through social media.
 - b) Email, texting, blogging and social media can encourage casual communication. Comments or posts intended to be humorous or informal may be misunderstood, taken out of context or shared more widely than intended.
 - c) Staff may be vulnerable to unintended misuse of information, photographs or other content.
 - d) Liking, sharing or commenting on another person's post may be interpreted as endorsing or supporting the views expressed.
 - e) Staff may be mentioned, tagged or identifiable in inappropriate posts, photographs or other online content without their knowledge or consent.
 - f) Online conduct does not have to relate directly to pupils in order to have implications for a member of staff's professional conduct or fitness to practise.
 - g) Content posted online is subject to the same laws relating to copyright, confidentiality and defamation as other forms of communication.
 - h) Inappropriate online behaviour may result in disciplinary, civil or criminal action.
- Staff who are members of professional organisations or trade unions are encouraged to seek appropriate advice and guidance regarding the responsible use of social media.

3. Privacy and Confidentiality

- Staff should be aware that personal information intended only for friends or family may become accessible to a much wider audience. Once information has been uploaded to the internet, it may be impossible to remove completely or control how widely it is shared.
- Many social media platforms provide privacy settings which allow users to restrict who can access their information. However, staff should not assume that privacy settings guarantee complete confidentiality.

Staff should:

- Familiarise themselves with the privacy settings of any social media platforms they use.
- Regularly review their privacy and security settings.
- Consider carefully what they post, share or comment on.
- Be aware that information can be copied, saved and shared by others.
- If a member of staff is unsure whether communication posted online could compromise their professionalism, reputation or relationship with the school community, they should carefully consider whether it is appropriate to post it.

- In particular, staff should be aware that:
 - a) Personal information can potentially be accessed by others. Social media platforms cannot guarantee complete privacy regardless of the settings used.
 - b) Once information is published online, control over that information may be lost. Other users may copy, share or comment on it.
 - c) Information posted anonymously can, in many cases, be traced back to its original source.
 - d) Photographs and other online content may contain location information which can be accessed by others.
 - e) Individual pieces of information may appear harmless but, when combined with other information available online, could potentially identify a pupil, parent/carers or member of the school community.
 - f) Staff must never share confidential or personal information relating to pupils, parents/carers, colleagues or the school.

4. Guidance for Personal Use

- Staff who have personal profiles on social media platforms should ensure that content, photographs, videos or other information available through those profiles does not:
 - a) Contain information that they would not be comfortable being viewed by colleagues, parents/carers or members of the wider community.
 - b) Undermine their position as a professional, trusted and responsible member of the school community.
- As a basic rule, if a member of staff would not be comfortable with colleagues, parents/carers or members of the school community seeing a particular comment, photograph, video or other content, they should not post it publicly online.

Staff should consider the following:

- a) Use appropriate privacy settings so that personal content is restricted to people they know and trust.
- b) Regularly review their friends/followers and connections.
- c) Staff should not accept friend or follow requests from current pupils.
- d) Staff should carefully consider whether accepting requests from parents/carers or other members of the school community through personal social media accounts is appropriate. Professional communication should take place through approved school channels.
- e) Personal blogs or websites should make it clear, where appropriate, that any views expressed are personal views and do not represent the views of St Joseph's RC Primary School.
- f) Staff should carefully consider the appropriateness of photographs, videos and other media posted on personal profiles and any potential impact they may have on individuals or the school.
- g) Information published online must comply with the school's confidentiality, data protection and safeguarding requirements. A breach of confidentiality may result in disciplinary action.
- h) Staff must always be respectful towards pupils, parents/carers, colleagues, the school, the Catholic community and members of the wider community.

- Staff should be aware that disrespectful, offensive, threatening or defamatory comments made online may result in disciplinary action.
- The school's name, logo, photographs, documents or other school materials should not be used on personal social media accounts without appropriate authorisation.
- Staff should remember that they may be perceived as representatives of the school outside of working hours. Images, posts, comments and other online activity can reflect upon both the individual and the reputation of St Joseph's RC Primary School.

5. Use of Official School Social Media Accounts

- St Joseph's RC Primary School may operate official social media accounts for the promotion of school activities, celebration of pupils' achievements and communication with parents/carers and the wider school community.
- The following principles apply to all official school social media accounts:
 - a) An official school social media account may only be established with the approval of the Headteacher.
 - b) Only authorised members of staff may access or post content to official school social media accounts.
 - c) Access to official accounts should be restricted to those members of staff who require it as part of their role.
 - d) Passwords and login information for official accounts must be kept confidential and must not be shared with unauthorised individuals.
 - e) Pupils must only be referenced, photographed or filmed in accordance with the school's permissions and procedures.
 - f) Photographs, videos or other media involving pupils must comply with the school's consent arrangements, safeguarding procedures and data protection requirements.
 - g) Personal information about pupils or families must not be published.
 - h) Copyright laws must be respected and sources appropriately acknowledged where required.
 - i) Content posted on official school accounts must be appropriate, professional, respectful and consistent with the Catholic ethos and values of the school.
 - j) Staff responsible for official accounts should ensure that content is checked before publication where appropriate.
 - k) Any member of staff who becomes aware of inappropriate or concerning activity on an official school social media account should report it immediately to the Headteacher or a member of the Senior Leadership Team.
- Failure to comply with these requirements may result in the matter being dealt with under the school's disciplinary procedures.

6. Use of IT Facilities in School

- All staff and pupils must adopt a responsible and common-sense approach to the use of IT facilities. This should include consideration of courtesy towards other users as well as compliance with legal, safeguarding and school requirements.
- The school's IT facilities, including computers, tablets, interactive screens, internet access, email systems and other digital resources, are provided primarily to support education, teaching, learning, administration and the effective operation of the school.
- Users should expect inappropriate or unacceptable use of school IT facilities to be addressed through the appropriate school procedures and, where necessary, disciplinary, safeguarding or legal action.
- Examples of inappropriate or unacceptable use include:
 - a) Using school IT facilities to intimidate, threaten, harass or offend another person.
 - b) Accessing, sending, downloading or sharing sexist, racist, discriminatory, defamatory, obscene, violent or otherwise inappropriate material using school IT facilities.
 - c) Deliberately introducing viruses, malware or other harmful software onto the school's network or devices.
 - d) Attempting to access another person's account, files or personal information without permission.
 - e) Violating the privacy of other users or deliberately disrupting their use of school IT facilities.
 - f) Using school equipment in a way that deliberately causes damage or loss.
 - g) Using school IT facilities for unauthorised private business, advertising or political purposes.
 - h) Installing software, applications or other programmes without appropriate permission.
 - i) Attempting to repair, alter, upgrade or otherwise interfere with school IT equipment without authorisation.
 - j) Using another person's username, password or account.
 - k) Attempting to bypass or disable the school's filtering, security or monitoring systems.
- This list is not intended to be exhaustive. Any use of school IT facilities that is considered inappropriate, unsafe, illegal or contrary to school policies may result in action being taken.
- Staff must comply with the school's Acceptable Use Agreement and all relevant Cardiff Council and/or local authority ICT requirements where applicable.
- Usernames and passwords are confidential and must not be shared with another person. Staff are responsible for activity carried out using their individual account and must report any suspected compromise of their account immediately.

7. Internet Filtering and Monitoring

- The school uses appropriate filtering and monitoring systems to help protect pupils and staff when using the internet and digital devices within school.
- Internet activity and searches may be monitored in accordance with safeguarding, data protection and legal requirements.
- Filtering and monitoring systems may identify searches, websites or online activity that present a potential safeguarding or online safety concern.
- If a member of staff or pupil encounters an unsuitable, inappropriate or concerning website or online material, this should be reported immediately to the Headteacher, Designated Safeguarding Person (DSP), member of the Senior Leadership Team or the person responsible for IT.
- The school will regularly review its filtering and monitoring arrangements to ensure that they remain appropriate and effective in protecting pupils and staff.

8. Communication and Awareness

- Online safety and acceptable IT use expectations will be communicated to staff and pupils through appropriate training, information and curriculum provision.
- Staff and pupils will be informed that network and internet use may be routinely monitored and that internet activity may be traceable to an individual user.
- Staff will be provided with clear procedures for reporting concerns relating to social media, internet use, IT misuse or online safety.
- The Social Networking and Acceptable IT Use Policy will be made available to all staff and will be accessible through the school's policy and staff documentation.
- Staff will be expected to familiarise themselves with this policy and comply with its requirements.

9. Handling E-Safety and Internet Misuse Complaints

- Complaints or concerns relating to internet misuse, social media or inappropriate IT use will be dealt with by the Headteacher or an appropriate member of the Senior Leadership Team.
- Where a concern relates to the safeguarding or welfare of a child, it must be dealt with in accordance with the school's Child Protection and Safeguarding Policy.

- Where appropriate, concerns may be referred to the school's Designated Safeguarding Person, local authority, Education Workforce Council, police or other relevant agency.
- Any investigation or subsequent action will be undertaken in accordance with the school's relevant policies and procedures, including disciplinary procedures where appropriate.

10. Review

This policy will be reviewed regularly to ensure that it reflects changes in technology, social media platforms, legislation, safeguarding requirements and school practice.

ALN

St Joseph's RC Primary School is committed to providing an inclusive learning environment in line with the Additional Learning Needs and Education Tribunal (Wales) Act 2018 and the ALN Code for Wales 2021. We are dedicated to identifying, assessing, and making provision for Additional Learning Needs at the earliest opportunity, working in collaboration with pupils, parents, and relevant professionals. Our approach is based on promoting equity, respecting diversity, and ensuring that all pupils are provided with opportunities to meet success.