Truro and Penwith Academy Trust

Social Media Policy

The following policy applies to all Truro & Penwith Academy Schools:

Alverton Primary School
Berrycoombe Primary School
Blackwater C.P. School
Bodriggy Academy
Cape Cornwall School
Cardinham School
Chacewater Primary School
Gulval School
Hayle Academy
Kehelland Village School
Kennall Vale School
Lanivet Community Primary School
Liskeard Hillfort School
Mithian School
Mousehole Primary School
Nancledra School
Newlyn School
Pendeen School
Pensans C.P. School
Perranporth C.P. School
Roche C.P. School
Sennen Primary School
St Dennis Primary Academy
St Erth School
St Ives School
St Just Primary School
Threemilestone School
Tywardreath School

DATE APPROVED BY TPAT Board of Trustees: May 2020
DATE FOR REVIEW: May 2023

September 2020 - 2023

Truro and Penwith
Academy Trust

Social Media Policy

1 INTRODUCTION

As a Truro and Penwith Academy Trust school, we ask that all TPAT schools and employees read through and follow this Social Media Policy. Employees of all TPAT schools may be able to access social media services and social networking websites at work, either through company IT systems or via their own equipment.

This social media policy describes the rules of social media use at any TPAT school. It sets out how employees must behave when using the school's social media accounts.

Why This Policy Exists

Social media can bring significant benefits to schools, particularly for building relationships with current and prospective staff, parents and students.

School social media policies have a number of purposes, but their overriding function is to protect staff, students and parents from the many issues that can arise as a result of posting on social networking sites.

Staff may be vulnerable to malicious and defamatory comments (and potentially even threats and abuse) from parents or pupils, and to allegations of grooming and other forms of online abuse. Twenty-one per cent of teachers say they've had derogatory remarks made about them online.

Parents may become involved in online disputes with other parents through social media. They may also potentially put their child and others within the school at risk by sharing photos, videos or other information that could make the children identifiable to others.

Pupils are at risk of cyber bullying and may also become involved in cyber bullying themselves. They are also vulnerable to other serious crimes such as grooming and abduction if they share too much personal information on social media.

Policy Scope

This policy is to be considered in conjunction with schools' own Acceptable Use of ICT policies and TPAT's Staff Code of Conduct.

This policy applies to all employees, contractors and volunteers at any TPAT school who use social media whilst at work – whether for business or personal reasons.

It applies no matter whether that social media activity takes place on school premises, while travelling for business or while working at home.

2 RESPONSIBILITIES

Everyone who operates a school social media account or who uses their personal social media accounts at work has some responsibility for implementing this policy.

The Headteacher is ultimately responsible for ensuring that the school uses social media safely, appropriately and in-line with the school and Trust's objectives.

However, these people have key responsibilities:

- Mrs. Watkins – Online safety lead
- Mrs. Courts – ensure that all parent consent is up to date.

3 SOCIAL MEDIA CONTENT

Content to be shared on social media must be related to your school and/or TPAT:

- Events and announcements
- Celebrations and successes
- Articles
- Press releases
- Photographs and videos
- Vacancies

The tone in which you deliver the schools' content on social media should be:

- Light-hearted
- Professional
- Dependent on content

4 GENERAL SOCIAL MEDIA GUIDELINES

Regardless of which social networks employees are using, following these simple rules helps to avoid the most common pitfalls:

- **Know the social network** – employees should spend time becoming familiar with the social network before contributing. It is important to understand what is and is not acceptable on a social media channel before posting anything
- **If unsure, don't post it** – staff should err on the side of caution when posting updates to social networks and if they feel that an update could cause offense or complaints, they should not post it, and should consult the Headteacher.
- **Be careful with images and personal information** – Employees should consult the Headteacher if unsure of the use of certain student images and should not include any

personal information when posting on the school website or social media accounts; full names, addresses, email addresses, phone numbers.

- **Keep a positive tone** – many social media users have gotten into trouble by simply failing to observe basic good manners online. Employees should adopt a pleasant tone when communicating online
- **Look out for security threats** – Staff should be on guard for social engineering and phishing attempts. Social networks can also be used for spam distribution and malware
- **Don't make promises without checking** – some social networks are very public so employees should not make any commitments or promises on behalf of the school or the trust without checking that the school can deliver on the promises. Direct any enquiries to the Headteacher
- **Don't escalate things** – it's easy to post a quick response to a contentious status update or query and then regret it. Employees should take the time to think before responding, and hold back if at all in doubt
- **Keep calm in a crisis** – unfortunately there are occasional incidents which require sensitivity (cyber-bullying, negative comments, external incidents) and it is important not to post on social media until you have the express permission of the Headteacher
- **Be careful with regards to students and staff –** do not accept friend requests from current or ex-students. You must notify the parent if a child sends you a friend request
- **Get permission –** written permission from parents or carers must be obtained before photographs of students or their work are published on the school website and social media
- **Appropriate photography –** Care must be taken when taking and using digital/video images. Students must be appropriately dressed and should not be participating in activities that might bring the individuals or the school into disrepute. Photographs published on the website, or elsewhere that include students, will be selected carefully and will comply with good practice guidance on the use of such images
- **Equipment use –** Images may only be taken on school equipment and the personal equipment of staff must not be used for such purposes

5 USE OF COMPANY ACCOUNTS

This part of the policy covers the use of social media accounts owned and run by the school.

Authorised Users

Only people who have been authorised to use the school's social networking accounts may do so. Authorisation is provided by the Headteacher. Allowing only designated people to use the accounts ensures the school's social media presence is consistent and in-line with guidelines.

Creating Social Media Accounts

New social media accounts in the school's name must not be created unless approved by the Headteacher. If there is a case to be made for opening a new account, employees should raise this with the Headteacher.

Inappropriate Content and Use

School social media accounts must not be used to share or spread inappropriate content, or to take part in any activities that could bring the school or TPAT into disrepute.

6 RESPONSIBLE USE OF SOCIAL MEDIA

Users must **NOT**:

- Create and distribute material that might be defamatory or incur liability for the school and/or TPAT
- Post message, status updates or links to material or content that is inappropriate
- Use social media for any illegal or criminal activities
- Broadcast their own views on social, political, religious or other non-school related matters
- Send offensive or harassing messages to others via social media
- Send or post messages that could damage the reputation or image of the school and/or TPAT
- Discuss colleagues, competitors, students or parents without their approval
- Accept friend requests from current or ex pupils
- Use the full names of students on the school or Trust website, social media or blog, particularly in association with photographs
- Publish photographs of students or their work without the permission of their parents or carers
- Take photographs on a mobile phone or any other personal item
- Use personal social networking sites or blogs when at work

Security and Data Protection

Users should maintain confidentiality and must **NOT**:

- Share or link to any content or information owned by the trust that could be considered confidential or commercially sensitive
- Share or link to any content or information owned by another school or person that could be considered confidential or commercially sensitive
- Share or link to data in any way that could breach the school's data protection policy

Protect Social Accounts

School social media accounts should be protected by strong passwords that are changed regularly, stored in a spreadsheet known to all involved parties, and shared only with authorised users

Staff must not use a new piece of software, app or service with any of the school's social media accounts without receiving approval from the Headteacher

7 POLICY ENFORCEMENT

Knowingly breaching this social media policy is a serious matter. Users who do so will be subject to disciplinary action.
Employees, contractors and other users of the school's social media mat also be held personally liable for violating this policy.

8 SIGNATURES

By signing below, I acknowledge that I have fully read and understood the Social Media Policy. I understand that if I have any questions or concerns about this policy, it is my responsibility to discuss this with the Headteacher.

Headteacher Name: _____

Signature: _____

Person Responsible Name: _____

Signature: _____

Person Responsible Name: _____

Signature: _____

Person Responsible Name: _____

Signature: _____

Person Responsible Name: _____

Signature: _____

Person Responsible Name: _____

Signature: _____

Person Responsible Name: _____

Signature: _____

Person Responsible Name: _____

Signature: _____

Person Responsible Name: _____

Signature: _____

Person Responsible Name: _____

Signature: _____

Person Responsible Name: _____

Signature: _____

Person Responsible Name: _____

Signature: _____

Person Responsible Name: _____

Signature: _____

Person Responsible Name: _____

Signature: _____

Person Responsible Name: _____

Signature: _____

Person Responsible Name: _____

Signature: _____

Person Responsible Name: _____

Signature: _____

Person Responsible Name: _____

Signature: _____

Person Responsible Name: _____

Signature: _____

Person Responsible Name: _____

Signature: _____