SOCIAL MEDIA POLICY

Introduction

The purpose of this document is intended to address the use in the trust by users (including but not limited to Employee, Students, Visitors, Contractors) of Social Media.

The trust recognises the numerous benefits and opportunities which a social media presence offers.

The trust aims to build relationships and work with the whole community to share news, information and successes. We will endeavour to use social media to engage appropriately with learners, collect feedback to gauge the student learning experience, enhance the trust profile within the community and in many ways yet to be discovered.

A social media account provides a flexible delivery platform. The trust will use it to supplement part of our communications but will restrict its use to officially authorised purposes such as communications via Marketing Department and IT Services. The trust will actively encourage our staff to make effective and appropriate use of it; to engage in conversations with colleagues and the community as well as sharing appropriate outputs.

In order to provide clarity and consistency for staff, while recognising the corresponding challenges for the trust, we have in place procedures to restrict use and some common sense boundaries. Our approach is therefore to support staff to engage with colleagues, learners and the community, while providing appropriate guidance and training on best practice.

Users are advised to refresh their knowledge of relevant policies which apply in this context, particularly the e-Safety Policy, ICT Acceptable Use Policy and Data Protection Policy.

1. Scope

For the purposes of this document, social media is defined as any online interactive communication tool which encourages participation and exchanges. Common examples include; Twitter, Facebook, YouTube, Skype, Instagram, Pinterest, and LinkedIn.

This document applies to all users and to all communications which directly or indirectly, represent the trust. It applies to online communications posted at any time and from anywhere, whether to an individual, a limited group or the world.

The Trust respects privacy and understands that users may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the institution's reputation are within the scope of this guidance.

Professional responsibilities apply regardless of the medium being used. All social media communications which might affect the trust's reputation, whether made either in a private or professional capacity, must comply with relevant trust policies which address user conduct.
Professional communications are those made through official channels, posted on an institutional account or using the trust name. All professional communications are within the scope of this document (and are subject to the ICT Acceptable Use Policy).

Personal communications are those made via a private social media account, such as a personal blog or wiki. In some limited circumstances these communications are subject to this document.

In all cases, where a private account is used which clearly identifies the trust it must be made clear that the user is not communicating on behalf of the trust. An appropriate disclaimer, such as:
"The views expressed here are my own and in no way reflect the views of the establishment" should be included.

Private communications which do not refer to the trust, are outside the scope of this document.
Digital communications with learners are also considered when appropriate.

Staff should refrain from accepting 'friend' requests from student except where the member of staff has a connection with the learner beyond the context of the institution.

2. Roles and Responsibilities

There are clear lines of responsibility for social media use within the Trust.
Central Services is responsible for

• Keeping up to date with technology developments through appropriate CPD
• Reviewing and updating all relevant documentation
• Delivering training and guidance on social media
• Taking a lead role in responding to and investigating any reported incidents
• Making an initial assessment when an incident is reporting and involving appropriate staff and external agencies as required

Marketing Department are responsible for
• Administrating and taking day to day ownership of all trust official Social Media accounts (where appropriate)
• Maintaining a directory of trust Social Media accounts and informing Central Services
• Addressing concerns or questions regarding posts or comments via official and personal accounts
• Reporting outcomes to Central Services, or escalating the matter to involve appropriate agencies
• Attending additional relevant training

Staff are responsible for
• Knowing the contents of this document and its procedures
• Ensuring that any use of social media is carried out in line with this and other relevant policies
• Attending appropriate training
• Informing Central Services where an institutional account is to be used
• Adding an appropriate disclaimer to personal accounts when naming the institution
• Reporting any incidents in line with section 5 below

3. Behaviour

The Trust requires that all users using social media adhere to the standard of behaviour as set out in this document and other relevant policies.

Users will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about other trust users.

Digital communications by users must be professional and respectful at all times and in accordance with this guidance. Where an incident is reported, refer to section 5 below. Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the trust and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate. The trust will take appropriate action when necessary.

Where conduct is found to be unacceptable, the trust will deal with the matter internally. Where conduct is considered illegal, the trust will report the matter to the police and other relevant external agencies, and may take action according to the Disciplinary Policy.

The HR Department may use social media for the purposes of recruitment selection.

The use of social media by users while at work may be monitored, in line with the relevant trust policies.

The Trust permits reasonable and appropriate access to private social media sites (via our Bring Your Own Device – BYOD Policy). However, where we suspect excessive use, and consider this use to be interfering with relevant duties, we may take disciplinary action.

4. Security

The Marketing Department are responsible for ensuring that passwords and other access controls for trust social media accounts are of adequate strength and kept secure. Passwords should be regularly changed in line with the trust policies and under no circumstances, should passwords be shared.

In regard to personal social media accounts, users should be familiar with privacy settings and ensure that these are appropriate for both content and intended audience.

Every effort will be made to keep security software up to date. Appropriate security measures will include the use of enhanced filtering and protection of firewalls, servers, routers, work stations etc. to prevent accidental or malicious access of IT systems and social media accounts. Digital communications, including via social media sites, over the trust network, will be monitored in line with the trust policies.

5. Incidents and Response

Any breach of this guidance could lead to disciplinary action. Where a breach of this guidance is reported to the trust this matter will be dealt with seriously and in line with the trust Disciplinary and ICT Acceptable Use policies. The trust will act immediately to prevent, as far as reasonably possible, any damage to an individual, their rights or the institution's reputation.

Any stakeholder or member of the public may report an incident to the institution. This should be directed immediately to IT Services or a relevant member of SMT.

Where it appears that a breach has taken place, IT Services or a relevant member of SMT will review what has happened and decide on the most appropriate and proportionate course of action.

Where the incident is considered to be serious, this will be reported to the Principal / Deputy Principal.

Where staff are in receipt of offensive, unacceptable content via social media, this should be reported to a relevant line manager immediately.

Where questionable content has been received by the institution, Central Services must be informed prior to any response being submitted.

This policy has been adopted by Churchward School:

Signed …….. Headteacher

Signed …….. Chair of Governors

Date ……