Social Media and Electronic Communication Policy

Oxford Schools Chaplaincy

Introduction

This policy sets out the standards expected of all OSC staff, volunteers and trustees when using social media and electronic communication in connection with OSC.

It is intended to minimise the safeguarding, wellbeing, data protection, professional and reputational risks associated with electronic communication, while enabling OSC to make appropriate use of digital communication.

This policy applies to everyone who works or volunteers for OSC, particularly those who have contact with children and young people through OSC's work in schools.

The Director is responsible for ensuring that new staff and volunteers are made aware of this policy as part of their induction.

This policy covers all forms of electronic communication, including but not limited to:

- email;
- WhatsApp and other instant messaging applications;
- Facebook and other social media platforms;
- mobile phones;
- website messages;
- online groups and communities;
- video conferencing and online meeting platforms; and
- other digital communication platforms that OSC may use in the future.

The principles in this policy should be applied to new technologies and platforms as they develop.

OSC's primary routes of communication with young people are through schools, teachers and face-to-face contact in appropriate public, classroom or group settings.

Electronic communication with young people should therefore only be used where there is a clear and legitimate OSC-related purpose.

Where communication relates to a church's own activities, the church's policies and procedures will normally apply. However, where an individual is acting in their capacity as an OSC staff member or volunteer, this OSC policy must be followed.

If there is uncertainty about which policy applies, advice should be sought from the Director.

General principles

Professional behaviour

Staff and volunteers are expected to maintain appropriate professional standards online as well as face-to-face.

Digital communication should reflect OSC's values and should not undermine the trust placed in OSC by young people, schools, parents, churches, volunteers or supporters.

Personal social media

OSC respects the right of staff and volunteers to use social media in their personal lives.

However, staff and volunteers should be aware that content posted on personal accounts may become associated with OSC where a connection to OSC can reasonably be identified.

Staff and volunteers must not post, share, encourage or link to material that:

- is abusive, threatening or harassing;
- is discriminatory or offensive;
- contains bullying or harassment;
- contains unlawful material;
- makes false or misleading statements about OSC;
- discloses confidential OSC, school or young people's information; or
- could reasonably bring OSC into serious disrepute.

Staff and volunteers should also consider that liking, sharing or otherwise promoting content may be interpreted as endorsing it.

Personal contact with young people

Staff and volunteers must not use personal social media accounts, personal email addresses or personal messaging accounts to communicate privately with young people under 18 whom they know through OSC.

They should not:

- accept friend or follow requests from young people they know through OSC on personal social media accounts;

- initiate private conversations with young people through personal social media;
- give young people their personal telephone number or personal email address; or
- ask young people for access to their personal social media accounts.

Where electronic communication with a young person is necessary for an OSC purpose, an OSC-authorised account, email address, work mobile phone or other approved communication method must be used.

Communication must be transparent

Communication with young people should, wherever reasonably possible, take place in a group or other transparent setting rather than through private one-to-one communication.

Where a one-to-one communication is genuinely necessary, there should be a clear OSC-related reason, an appropriate record of the communication, and appropriate oversight in accordance with OSC safeguarding procedures.

Purpose of communication

Electronic communication with young people should only be used for genuine OSC-related purposes, such as:

- arranging meetings;
- providing information about OSC activities;
- communicating practical information about CU or CU leadership activities; or
- other activities specifically authorised by OSC.

It must not be used to develop or maintain a personal relationship with a young person.

Appropriate timing

Staff and volunteers should avoid initiating or responding to communication with young people outside reasonable working or activity hours.

As a general expectation, communication should not take place between **9pm and 8am**, unless there is an immediate safeguarding concern or another exceptional circumstance requiring urgent action.

Language and tone

Staff and volunteers must take care with the language used in electronic communication.

Messages should be professional, clear and appropriate to the age and circumstances of the young person.

Particular care should be taken with informal language, emojis, abbreviations, humour and comments that could be misunderstood when read without the context of a face-to-face conversation.

Image and videos

Photographs and videos of children and young people must only be taken, stored or published in accordance with OSC's safeguarding, consent and data protection requirements.

Staff and volunteers must not use personal devices or personal accounts to store or share photographs of young people for OSC purposes unless specifically authorised in accordance with OSC procedures.

Church relationships

Staff and volunteers may know young people through their church as well as through OSC.

Where someone is acting in a church capacity, the church's policies apply to that communication.

However, staff and volunteers should remain aware of the potential for blurred boundaries and should seek advice from the Director if a dual relationship creates a safeguarding or professional boundary concern.

Existing personal relationships

If an OSC staff member or volunteer already knows a young person personally, for example because the young person is their child, a family friend or the child of a friend, this should be disclosed to the Director where it could affect their work with that young person through OSC.

Appropriate arrangements should then be agreed to maintain transparency and professional boundaries.

Young people who reach 18

Turning 18 does not automatically mean that all professional boundaries cease to apply.

Where a young person has left school and is 18 or over, communication through personal social media, email or telephone may be appropriate, provided there is no continuing safeguarding or other reason why this would be inappropriate.

Staff and volunteers should continue to maintain appropriate professional boundaries and should consider the individual's circumstances before changing the method of communication.

Safeguarding

This policy must be read alongside OSC's Safeguarding Policy and Procedures. The safeguarding requirements apply equally to face-to-face and electronic communication, including social media, messaging, online groups and video conferencing.

Any safeguarding concern, allegation, disclosure or worrying communication involving a child or young person must be dealt with in accordance with OSC's safeguarding procedures.

Staff and volunteers must **act immediately on safeguarding concerns and must not delay reporting them**.

Where a concern relates to a young person in school, the concern should be passed to the appropriate Designated Safeguarding Lead (DSL) at the school in accordance with the school's procedures, and to the OSC Director as required by OSC's Safeguarding Policy.

If a child is in immediate danger, the appropriate emergency safeguarding arrangements must be followed.

Once a safeguarding concern or allegation has been raised, staff and volunteers must not investigate it themselves through social media, messaging or other electronic communication.

They should not question other young people, attempt to obtain explanations, or discuss the matter informally online.

Relevant electronic messages should be retained where they may be necessary as evidence of a safeguarding concern, complaint or other matter.

Staff should not unnecessarily forward, copy or distribute safeguarding material.

Any recording or sharing of information must comply with OSC's GDPR and safeguarding procedures.

Social Media

OSC may maintain official social media accounts to:

- promote OSC activities and events;
- communicate with supporters and supporting churches;
- share appropriate news and information;
- promote relevant events run by churches and other organisations; and
- support OSC's vision and programme.

Access to OSC social media accounts will be restricted to authorised staff or other people specifically approved by the Director.

Official accounts should be used rather than personal accounts when posting on behalf of OSC.

Messages received through OSC social media accounts should be dealt with promptly and appropriately.

Where a message raises a safeguarding concern, staff must follow OSC safeguarding procedures rather than attempting to resolve the matter through social media.

Personal accounts should not be used to establish private online relationships with young people known through OSC.

Staff and volunteers should be particularly cautious about accepting friend requests, follows or direct messages from young people.

Email

OSC email addresses should be used for OSC business wherever possible.

Staff and volunteers should not use personal email accounts to communicate privately with young people on behalf of OSC.

Where an OSC staff member needs to email a young person for a legitimate OSC purpose, this should normally be done using an OSC-authorised email address and, where appropriate, a school email address.

Communication should be transparent and appropriate to the purpose for which the email address was obtained.

Young people's email addresses and other personal information must only be collected and used where there is a legitimate OSC purpose and appropriate permission or other lawful basis.

Personal information must not be used for purposes unrelated to the reason for which it was obtained.

Emails containing sensitive or confidential information should be handled in accordance with OSC's GDPR Policy.

WhatsApp and direct messaging

WhatsApp and similar messaging applications may only be used with young people in accordance with the **OSC WhatsApp Guidelines**.

Communication with young people through WhatsApp must use an OSC work mobile phone or other OSC-authorised account.

Personal mobile phones must not be used for direct communication with young people on behalf of OSC.

Where WhatsApp is used with young people, group communication should be used wherever reasonably practicable.

The relevant OSC staff member should administer the group and ensure that appropriate safeguards are in place.

Private messaging with individual young people should not be initiated by OSC staff or volunteers.

If a young person sends a private message, the staff member should follow the procedures in the OSC WhatsApp Guidelines and consider whether the communication needs to be brought into an appropriate group or made visible to another responsible adult.

OSC volunteers are not permitted to communicate directly with young people under 18 through WhatsApp or other personal messaging services on behalf of OSC unless specifically authorised under OSC's procedures.

Mobile phones

Personal telephone numbers should not be given to young people for OSC purposes.

Communication with young people by telephone should normally take place through an OSC work mobile phone or other OSC-authorised communication method.

Where a young person contacts an OSC staff member through a personal number unexpectedly, the staff member should avoid continuing the communication through that personal number and should move the communication to an appropriate OSC-authorised channel.

Staff and volunteers should not use personal devices to photograph, record or store images or personal information about young people for OSC purposes unless specifically authorised and handled in accordance with OSC's safeguarding and GDPR procedures.

Online groups and moderation

Any OSC online group involving young people should have a clear purpose, appropriate membership and an identified person responsible for moderation.

The person responsible for the group should understand how to:

- moderate content;
- remove inappropriate material;
- manage membership;
- identify safeguarding concerns; and
- report concerns through OSC's safeguarding procedures.

Where an online group is being used for a live session or meeting with children or young people, the requirements set out in the **Online meetings and video conferencing** section of this policy must also be followed.

The person responsible for administering an online group does not necessarily need to be the person leading a live session. However, where children or young people are participating in a live online session, OSC's requirements regarding the presence of appropriately recruited and safeguarding-checked adults must be followed.

Online meetings and video conferencing

OSC may use video conferencing and online meeting platforms to support its work with children and young people where there is a clear and legitimate OSC-related purpose.

Any online meeting involving children or young people must be planned and conducted in accordance with OSC's Safeguarding Policy and Procedures and this policy.

Approved platforms

Only platforms approved by OSC should be used for online meetings with children and young people. Before using a platform, consideration should be given to its safeguarding, privacy, data protection, security and moderation features.

Staff and volunteers should not introduce a new platform for communication with young people without first obtaining approval from the Director.

Adult supervision

Where an online meeting involves children or young people, at least two appropriately recruited and safeguarding-checked adult leaders should be present wherever reasonably practicable.

Both adult leaders should join the meeting before young people are admitted. If there are insufficient appropriately recruited adults to run a meeting safely, the meeting should not proceed without first discussing the situation with the Director.

Parental awareness and consent

Parents or carers should be informed in advance of online meetings involving their child and, where required by OSC's safeguarding procedures, their consent should be obtained.

Meeting invitations and joining information should normally be sent to parents or carers rather than directly to young people, unless an alternative arrangement has been specifically agreed with the parent or carer and is consistent with OSC procedures.

Records of consent should be retained in accordance with OSC's GDPR Policy.

Online environment

Young people should be encouraged to participate from an appropriate shared or communal area of their home wherever reasonably practicable. They should not normally participate from their bedroom.

Adult leaders should follow the same principle and should take reasonable steps to protect the privacy of other people in their home.

If a young person's camera shows an inappropriate or private environment, the leader should ask them to move to a more appropriate location or switch off their video.

Communication and boundaries

The same professional boundaries that apply to face-to-face work apply to online meetings.

Communication should remain focused on the purpose of the meeting and should not be used to develop or maintain inappropriate personal relationships with young people.

Private messaging between adult leaders and individual young people should not be used during an online meeting unless there is a specific safeguarding reason and the communication is handled in accordance with OSC safeguarding procedures.

Where reasonably practicable, the platform should be configured so that private messaging between participants is disabled.

Meeting security

Online meetings should use appropriate security measures, which may include:

- a meeting password or other access control;
- a waiting room or equivalent function;
- restricting screen sharing to the host or authorised adult leaders;
- restricting file sharing or file transfer where the platform allows this;
- limiting participants to those who have been invited; and
- ensuring that appropriate moderation controls are available.

Meeting links, passwords and joining information should not be shared publicly.

If an unauthorised person enters a meeting, the host should remove them promptly and use the platform's security controls to prevent further disruption. If inappropriate or disturbing material is displayed or shared, the meeting should be paused or ended if necessary and the incident reported in accordance with OSC's safeguarding procedures.

Recording

Online meetings involving children and young people must not be recorded unless OSC has specifically authorised the recording in advance and all necessary safeguarding, consent, data protection and storage requirements have been addressed.

Screenshots, photographs or copies of chat messages must not be taken or retained unless there is a legitimate reason and this is permitted under OSC's safeguarding and GDPR procedures.

Chat and participant interaction

Where a chat facility is used, private messaging should be disabled wherever the platform permits this.

Adult leaders should monitor the chat during the meeting and respond appropriately to inappropriate or concerning messages.

If a young person appears upset, unwell or distressed during an online meeting, an adult leader should respond appropriately and, where necessary, contact the parent or carer and follow OSC's safeguarding procedures.

Any safeguarding concern, disclosure or allegation arising during an online meeting must be dealt with in accordance with OSC's Safeguarding Policy and Procedures.

Technical support and inclusion

Adult leaders should familiarise themselves with the platform before using it with young people and should consider accessibility and technical difficulties that may prevent a young person from participating.

OSC should consider reasonable ways of supporting young people who do not have suitable technology, internet access or a suitable environment in which to participate.

Dynamic risk assessment

Online meetings should be subject to an appropriate risk assessment. Adult leaders should remain alert to new safeguarding, privacy, technical and wellbeing risks and should report significant concerns or emerging risks to the Director so that OSC's arrangements can be reviewed.

Data protection and confidentiality

Staff and volunteers must comply with OSC's GDPR Policy when using social media and electronic communication.

Confidential information must not be posted or shared through personal social media accounts or inappropriate messaging channels.

This includes information about:

- young people;
- families;
- schools;
- safeguarding concerns;
- staff and volunteers;
- internal OSC matters; and
- information intended only for internal use.

Electronic communication should only contain information that is necessary and appropriate for the purpose.

Technology changes

Electronic communication is continually changing. New social media platforms, messaging services and digital technologies may become relevant to OSC.

The principles of this policy apply to new platforms even where they are not specifically named.

Before using a new platform to communicate with young people on behalf of OSC, staff should consider:

- safeguarding risks;
- privacy and data protection;
- age requirements;
- whether an organisational account or device can be used;
- moderation arrangements;
- how records will be retained; and
- whether the platform is appropriate for the intended purpose.

Where there is uncertainty, advice should be sought from the Director before communication with young people begins.

Breaches of this policy

All OSC staff and volunteers are expected to comply with this policy.

A breach may result in action being taken under the relevant OSC procedures.

For employees, this may include the organisation's disciplinary procedure where appropriate.

For volunteers, serious or repeated breaches may result in the volunteer being asked to stop volunteering with OSC.

Any breach involving a safeguarding concern will be dealt with in accordance with OSC's Safeguarding Policy and Procedures.



Review

This policy will be reviewed annually, or sooner if there are significant changes to:

- safeguarding guidance;
- data protection requirements;
- relevant legislation;
- social media or messaging technology; or
- OSC's activities and working practices.