

**SOCIAL MEDIA POLICY**

**Contents**

[1. Introduction 1](#_Toc114761176)

[2. Scope 1](#_Toc114761177)

[3. Purpose 1](#_Toc114761178)

[4. Risk 1](#_Toc114761179)

[5. Responsibilities 2](#_Toc114761180)

[6. Social Messaging Apps 2](#_Toc114761181)

[7. Approved Use 2](#_Toc114761182)

[8. Appropriate Use 3](#_Toc114761183)

[9. Group Messaging 3](#_Toc114761184)

[10. Media 4](#_Toc114761185)

[11. Monitoring 4](#_Toc114761186)

[12. Retention 4](#_Toc114761187)

[13. Data Subject Rights 4](#_Toc114761188)

[14. Personal Data Breaches 5](#_Toc114761189)

[15. Disciplinary Action 5](#_Toc114761190)

[Annex A – Social Media Guidelines A-1](#_Toc114761191)

[Annex B – Social Media Group Application B-1](#_Toc114761192)

# Introduction

## This policy forms part of the technical and organisational measures implemented by Jesus College (‘the College’) to ensure its processing of personal data is performed in accordance with the provisions of the Data Protection Act 2018 (DPA 2018) and UK General Data Protection Regulation (UK GDPR). It should be read in conjunction with other internal policies and procedures including, but not limited to, the General Data Protection Policy, Acceptable Use Policy, Remote Working Policy, and Personal Data Breach Policy.

## Social media can bring enormous benefits and opportunities to an academic community, including by enabling global communication and collaboration, and promoting healthy and lively academic debate. There is, however, an inherent risk involved in using social media, in that it is an instantaneous and far-reaching form of communication and inappropriate use has the potential to cause serious, and sometimes unexpected and long-term, consequences. We encourage all College members to engage, collaborate and innovate through social media; however, wherever and however this is done, they must be aware of the potential impact on themselves and other users.

## 1.3 This policy aims to minimise the risks of using social media and messaging apps inappropriately which can impact on the wellbeing of staff and the reputation of the College, so that staff can enjoy the benefits of social networking and messaging whilst adhering to the standards expected by the College.

# Scope

2.1 For the purpose of this policy, *social media* is any online interactive tool which encourages participation, interaction and exchanges, such as blogs, discussion forums, instant messaging and any website that allows public commenting or posting. Current popular platforms include Facebook, Instagram, YouTube, LinkedIn, WhatsApp, Snapchat, TikTok and Twitter.

## This policy applies to all College members who create, contribute to, or communicate digitally using online interactive tools, and to all forms of social media and social messaging that have the potential to impact the College, whether during working hours or otherwise, and whether social media is accessed using issued equipment i.e. iPhones, tablets, laptops etc., or equipment belonging to members of staff or a third party.

# 3. FREEDOM OF SPEECH

## Freedom of speech and academic freedom are central tenets of college and university life, including in a social media context, and nothing in this guidance is intended to compromise these fundamental freedoms. Please refer to the [College Code of Practice for the protection of Freedom of Speech](https://www.jesus.ox.ac.uk/wp-content/uploads/2021/03/FOS-Code-of-Practice-July-2016.pdf) for the College’s definition and policy regarding free speech.

# Risk

## The College recognises the benefits of staff engaging and collaborating through social media /social messaging; however, whenever a member of staff does so, they must be aware of the potential risks and impact to both themselves and the College.

## The inherent risk involved in using social media and social messaging apps is that these communications can fall outside the normal governance and oversight of the College. They are an instantaneous and far-reaching form of communication, and the inappropriate use of social media and social messaging apps can have a direct impact on staff and other members of the community and cause reputational damage to the College.

## Staff should be aware of security threats and be on alert to social engineering and phishing attempts. Social networks can also be used to distribute spam and malware.

## The content of messages is also potentially disclosable should the College receive a Subject Access Request ([see section 14](#_Data_Subject_Rights)).

# Responsibilities

## Staff are responsible for their words and actions in an online environment and are therefore advised to consider whether any comment, photograph, or video they are about to post or share on a social networking or social messaging app, is appropriate (see Social Media Guidelines at [Annex A](#_Annex_A_–)).

## When using social media for work purposes, staff should use their true identity i.e. state their real name and their role, and reveal who they work for, especially if they are posting about the College or offering comments about a competitor.

## Line managers are responsible for addressing any concerns and/or questions about the use of social media and social messaging apps. They should avoid using social media and social messaging apps to discuss sensitive issues with their staff i.e. health related absences etc. Where doing so is unavoidable, the ‘chat’ is to be saved to the corporate record as expeditiously as possible so as to preserve a record of the conversation.

## Group administrators are responsible for the conduct and behaviour of staff in a ‘Group Chat’ and for the administration of the group i.e. adding/removing joiners and leavers.

## The Communications Manager is responsible for giving specialist advice on the use of social media for business related purposes.

# Social Messaging Apps

## Types of social messaging applications (apps) include, but are not limited to: WhatsApp, Instagram, Snapchat, Signal, Tik Tok, YouTube, Facebook, Twitter, LinkedIn, etc.

## Some apps i.e. WhatsApp, are end-to-end encrypted meaning that each message has a unique ‘lock and key’, that keeps the content confidential to the extent that not even the service provider is able to see the content of the messages exchanged.

## Staff are to adhere to the social media platform’s Acceptable Use Policy when accessing social media and messaging apps for either work-related purposes or personal reasons on handheld devices issued by the College.

# Approved Use

## Staff must not use their work email addresses to register on social networks, post blogs or other online tools that are utilised purely for their own personal use.

## Before any publicly available messaging app can be used for work purposes it must:

1. be approved by a line manager who will review of the app’s Terms and Conditions to understand how the information is processed, where the information is stored, and the security arrangements are in place in terms of third-party access.
2. the College’s IT Team will assess the security and access controls available on the app to confirm the apps suitability to be used for work purposes.

## Approved social messaging apps can be accessed on devices issued by the College or on a personal device i.e. a device owned by a member of staff e.g. an iPhone.

## Access to a messaging app downloaded to a handheld device is to be secured using any of the following methods: password, pin, fingerprint, voice, or facial recognition.

# Appropriate Use

## Worktime. Staff should refrain from using equipment provided by the College to access social media while at work unless authorised to do so by a manager.

## Personal opinions. Staff should only comment within their own area of expertise, and they should never represent themselves as a spokesperson for the College unless that is within their role and function.

## Confidentiality. Staff should maintain the confidentiality of the College’s commercially sensitive, private, or confidential information. Staff should ask permission from their line manager or a College Officer to publish or share internal reports, policies, procedures, or other internal business-related confidential communications on social media.

## Sensitive topics. Staff should seek guidance from the Communications Manager before posting anything that may be considered sensitive that may impact the College’ reputation.

## Honest and accurate. Staff should always be honest and accurate when posting information or news: if a mistake is made, it must be rectified quickly.

## Fair and courteous. Staff should always be fair and courteous to their co-workers, customers, suppliers, and the people who work on behalf of the College. Staff should not post statements, photographs, video, or audio that could be viewed as malicious, obscene, threatening or intimidating, that disparages co-workers, customers, or suppliers, or that might constitute harassment or bullying. Further information on this can be found in the [Jesus College Policy and Procedure on Harassment](https://www.jesus.ox.ac.uk/wp-content/uploads/2022/02/Jesus-Harassment-policy-and-procedure-FINAL.pdf).

## Disclaimer. Staff should make it clear when publishing a blog or posting online about their work or subjects associated with the College, that they are not speaking on behalf of the College. It is best to include a disclaimer such as "The postings on this site are my own and do not necessarily reflect the views of the College." All statements must be true and not misleading; all claims must be substantiated.

## The College reserves the right to take appropriate disciplinary action against any member of staff whose use of social media or social messaging is considered to be derogatory, discriminatory, bullying, threatening, defamatory, offensive, intimidating, harassing, creating legal liability for the College, or brings the College into disrepute.

# Group Messaging

## An ‘Administrator’ will need to be appointed before a ‘Group’ can be set-up on any approved social messaging app (see previous section). The appointed administrator is to complete the Social Media Group Application at [Annex B](#_Annex_B_–), and send the application to their line manager for approval.

## For some groups, it may be appropriate to appoint an assistant administrator to cover those periods when the Group administrator is unavailable.

## As soon as the Group becomes active, the appointed administer(s) is to ensure that:

1. only current members of staff are accepted into the Group;
2. personal data is not routinely processed by group members on the messaging app.
3. special category personal data i.e. health data, are not exchanged in ‘Group chat’;
4. only the minimum amount of personal data is shared on the messaging app.
5. relevant information is transferred to the corporate record as soon as possible;
6. conversations are monitored and inappropriate behaviour is challenged
7. conversations are held for no more than 7 days before being deleted;
8. access to the Group ceases when a member:
9. is excluded from the Group; or,
10. elects to leave the Group; or,
11. ceases to be an employee of the College;

## Group members are to ensure that any device used to access the Group is secured ([see section 7](#_Authorised_Use) above) and that the ‘group chat’ is not left open for others to see.

## Conversations are not to be discussed with ‘non-members’ of the Group or otherwise made available i.e. by allowing others to see the chat or by forwarding or copying the chat to a different platform. Doing so, will be considered a breach of confidentiality and may, in some circumstances, amount to a personal data breach ([see section 14](#_Personal_Data_Breaches)).

# Media

## Staff should not speak to the media on behalf of the College unless authorised to do so. All media inquiries are to be directed to the Communications Manager.

# Monitoring

## Where appropriate, the College reserves the right to monitor the use of social media and approved social messaging apps and to take appropriate action to protect itself against any misuse that may be harmful to the College.

## The College may review social media and social media messages shared by staff to identify any content that might be unlawful or otherwise has the potential to adversely impact another individual, be they co-worker or otherwise, or cause reputational damage.

## The College reserves the right to monitor usage and archive social media records including conversations on approved social messaging apps i.e. group chats.

# Retention

## Corporate communications are deleted in accordance with the time periods set out in the Record Retention & Disposal (RR&D) Schedule. It is the responsibility of the Group Administrator(s) to delete ‘Group Chat’ after 7 days.

## Conversations on approved social media messaging apps e.g. WhatsApp (see [section 7](#_Approved_Use) above) are not to be backed up to the Cloud.

# Data Subject Rights

## When responding to a subject access request (SAR), the College must provide access to any information it holds about a person, subject to any lawful exemptions or restrictions that might apply. This may include social media or conversations obtained from an approved social messaging app used for work purposes. For more information on Data Subject Rights, see Page 5 of the College’s [General Data Protection Policy](https://www.jesus.ox.ac.uk/wp-content/uploads/2021/12/Jesus-College-Data-Protection-Policy-November-2021.pdf).

# Personal Data Breaches

## A personal data breach is a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject

## Any loss/suspected loss, or any unauthorised use or suspected unauthorised disclosure of personal data through social media or an approved messaging app must be reported in accordance with the ‘Personal Data Breach Policy’.

## Personal data breaches may be reported to the Information Commissioner’s Office (ICO).

# Disciplinary Action

## Staff are to adhere to this policy and its intent. Failure to do so may result in disciplinary action being taken. Such action might include written or verbal warnings or instant dismissal in circumstances that amount to gross misconduct. For instance:

1. Using social media platforms to send confidential data without authorisation.
2. Sending offensive or inappropriate messages to customers, colleagues, or partners.
3. Using social media platforms or approved messaging apps for an illegal activity.

## The College may require staff to remove social media posts or conversations on approved social messaging apps which constitute a breach of the standards set out in this policy. Failure to comply with such requests may, in itself, result in disciplinary action.

## The College reserves the right to take appropriate disciplinary action against contractors and self-employed service providers who fail to comply with this policy. Such actions include, but are not limited to, the termination of any contract with the College.

## Using social media to post offensive or abusive comments, images or other content may also constitute a breach of The University Code of Discipline. Using social media to post offensive comments, images or other content may be a breach of the Code of Discipline under Statute XI and could result in disciplinary action by the Proctors. Such material could constitute:

* "harassment” under Section 2(m) of the Code of Discipline, as defined in the University’s Harassment Policy
* a breach of section 2(h) of the Code of Discipline: engaging in “violent, indecent disorderly, threatening or offensive behaviour or language

# 15.5 Social Media and Professional Courses

#  In addition, if you are taking a course which will result in a professional qualification (such as teaching, medicine or law) you may have to meet standards of behaviour set by the national professional body or by an institution you are working for (eg a school for students on the PGCE), or by the University under the Fitness to Practice or Fitness to Teach regulations. 3 These rules may expect you to uphold the reputation of the profession, or of an institution and so may cover a very broad range of conduct, including conduct which would otherwise be acceptable. An example could be a PGCE student posting criticism on Facebook about the partnership school he or she had been placed with. Content you post on social media could result in you being in breach of these rules and if serious could result in you losing the opportunity to pursue your chosen profession. IT Regulations – this page from IT Services contains links to all of the University’s Regulations, Information and Guidance relating to the use of University IT and communications facilities, which may also be applicable when it comes to social media and online content.

Annex:

1. Social Media Guidelines.
2. Social Media Group Application Form.

# Annex A – Social Media Guidelines

At Jesus College, we understand that social media can be an easy way to share your life and opinions with family, friends, and co-workers around the world. However, use of social media also presents certain risks, and carries with it certain responsibilities.

To assist you in making responsible decisions about your use of social media, we have established these guidelines for appropriate use of social media.

* Staff should be able to enjoy the benefits of social networking whilst understanding the standards of conduct expected by the College.
* Staff and staff should apply the same standards of conduct online as they are expected to apply offline.
* Staff should be familiar with privacy settings of social networking platforms, and should ensure that these are appropriate for both content and intended audience.
* Social networking platforms are in the public domain, and it is not always possible to be sure what is being viewed, shared, or archived, even if material is posted on a closed profile or group. There can be no reasonable expectation that posts will remain private and will not be passed on to other people, intentionally or otherwise. Material published online may have the potential to be available publicly, indefinitely.
* Staff are responsible for their words and actions in an online environment and are therefore advised to consider their use of language and phrasing, and whether any comment, photograph, or video they are about to post on a social networking site is something they would want fellow staff, colleagues, managers, members and/or people outside of the College to see.
* Inappropriate behaviour via social media may constitute harassment and bullying and can be reported to your line manager and/or a College officer.
* The College recognises that members of staff may occasionally wish to use social media for personal use at their place of work, by means of the College’s computers, networks and other IT resources and communications systems. Such incidental and occasional use of these systems is permitted, provided that: it is not excessive, does not disrupt, distract or is intrusive to the conduct of the College business and/or work colleagues (for example, due to volume, frequency, or cost), such communications do not bring the College into disrepute.
* Staff should not post messages, status updates or links to material or content which is deemed to be inappropriate by the College. Such content includes, but is not limited to: pornography, racial or religious slurs, gender-specific comments, information encouraging criminal skills or terrorism or materials relating to cults, gambling or illegal drugs. Inappropriate content or material also covers any text, images or other media that would reasonably offend someone on the basis of race, age, sex, religion or belief, disability, sexual orientation, gender reassignment, marriage or civil partnership, pregnancy and maternity or any other characteristic protected by law.
* Staff have the right to freedom of thought, opinion and expression and can use social media as a means of communicating these. However, staff should be aware that when posting on social media or forwarding/publishing other's opinions or articles for academic debate (e.g. re-tweeting) then the same requirements on not posting or linking to inappropriate content still apply.
* The College does not directly monitor the social media accounts of staff. However, the College does monitor social media for mentions of the College and other topics of relevance, so that we can respond directly to those who are raising questions or concerns about the College that we may be able to answer. As might be expected, posts by staff may appear as part of this monitoring. the College also uses Twitter lists and keyword searches to identify posts from the College departmental or staff accounts that we might helpfully promote or repost from the main corporate accounts.
* When disagreeing with others’ opinions, remain appropriate and polite. If you find yourself in a situation online that looks as if it may be becoming antagonistic, do not get overly defensive and do not disengage from the conversation abruptly; ask the Communications Manager for advice and/or disengage from the dialogue in a polite manner that reflects well on the College.
* Never comment on anything related to legal matters, litigation, or any parties the College may be in dispute with.
* If you are concerned that there has been a misuse of social media by another colleague, then you can report this to your line manager.
* Be smart about protecting yourself, your privacy, and the College’s confidential information. What you publish is widely accessible and will be around for a long time, so consider the content carefully.

# Annex B – Social Media Group Application

**To be completed by the Group Administrator**

|  |  |  |
| --- | --- | --- |
|  | **Group Administrator** | **Assistant Administrator** |
| Name: |  |  |
| Position: |  |  |
| Department: |  |  |

**Group**

|  |  |
| --- | --- |
| Group Name: |  |
| Purpose: |  |
| Social Media Application: | i.e. WhatsApp |
| Membership: | [Insert team, section, shift, club etc.] |

**Declaration**

|  |
| --- |
| As an Administrator from the Group, I will ensure that:* only current members of staff are accepted into Group
* personal data is not routinely processed by Group members
* special category personal data i.e. health data, is not discussed in group chat
* only the minimum amount of personal data will be shared on the messaging app
* relevant information is transferred to the corporate record as soon as possible
* conversations are monitored and inappropriate behaviour is challenged
* conversations are stored for no more than 7 days before being deleted
* access to the Group ceases when a member:
* is excluded from the Group; or,
* elects to leave the Group; or,
* ceases to be a member of staff
 |
| I have read and understood the ‘Social Media Policy’, ‘Acceptable Use Policy’ and ‘Remote Working Policy’, and I agree to abide by the provisions contained therein.  |
| **Group Administrator** | **Assistant Administrator** |
| [Signature] | [Date] | [Signature] | [Date] |

|  |  |
| --- | --- |
| **Approved by 1st Line Manager** | **Authorised by 2nd Line Manager** |
| Name: |  | Name: |  |
| Department: |  | Department: |  |
| Signature: |  | Signature: |  |
| Date: |  | Date: |  |