



Microsoft Teams Chat Policy (Surrey and Sussex) (1234/2026)

Abstract

The intention of this policy is to provide clear instruction to ensure users are aware of the safe and secure use of Microsoft Teams Chat. It is the responsibility of every Microsoft Teams user to know this policy and to conduct their activities accordingly.

Policy

1. Introduction

1.1 This policy and associated procedure apply to all users entitled to access Microsoft Teams Chat (hereon referred to as Teams Chat). Teams Chat is the native instant messaging application within the Microsoft Teams collaboration platform which combines video conferencing, call function, voicemail, instant messaging, screen sharing, file storage and application sharing.

It is an application hosted in the Forces' Microsoft 365 Cloud tenant and integrates with SharePoint Online, OneDrive as well as Outlook (Exchange online). Access to, and use of, Microsoft Teams will only be granted once vetting has been completed and a Force account has been issued and migrated to Cloud services.

1.2 Teams Chat provides an instant messaging capability which can be accessed from Force devices, including Mobile Data Terminals (MDTs). This functionality is designed for both internal and external use with organisations which subscribe to Microsoft Teams and have been granted guest access to our Cloud.

2. Scope

2.1 This policy and procedure cover all information conveyed over the Microsoft Teams platform and it is the responsibility of every Microsoft Teams user to know this procedure and to conduct their activities accordingly when utilising the Chat functionality.

3. Policy Statement

3.1 Microsoft Teams is to be used to collaborate with colleagues within Surrey Police and Sussex Police and approved third parties.

Procedure

1. Definitions

1.1 • Teams Chat Instant Messaging – real time one to one / one to many (group chat / channel posts / meeting conversations).

- Presence States - a combination of colour indicator and text string to indicate users' availability.
- Document Sharing - the ability to share a document for collaborative working within a Chat file library or as a link / attachment.
- Desktop Sharing - the ability to show another user your screen content as you see it.
- Voice Calling - one to one / group call voice communication between users.
- Video Calling - one to one / group call - visual communication between users.
- Multi-party Conversation / Conference - the ability to hold a multi-person voice or visual communication session.
- Externally Hosted Teams Meetings - users can join Microsoft Teams hosted by other forces and organisations and participate in their Teams and meeting Chat.
- Send to Outlook – individual segments of a Teams Chat can be exported and populated into an email via the 'share to Outlook' option, and vice versa.

2. General principles of instant messaging via Teams Chat

2.1 Chat (instant messaging) is a key business tool for communication hosted on a Cloud service assured to OFFICIAL with a handling caveat of SENSITIVE. Any conversation or information exchanged across the Teams Application, whether via Teams Chat or Teams meetings / calls, can form part of the corporate record and could be used as evidence in legal proceedings. Misuse of Teams Chat could result in disciplinary or even legal action being taken against individuals and the Force. Please see section 5 for further guidance.

2.2 Any Teams Chat messages could be used as part of a contractual agreement / obligation or even as evidence in court for criminal and harassment proceedings. You will be personally accountable for any content or attachments you send over Teams Chat. Only use text that you could personally justify, for example, if read out in court.

2.3 Users should regularly check their Microsoft Teams account for new Chat messages and maintain their availability status.

2.4 Care must be taken when sending Teams Chat messages. Users must ensure that the correct recipient is selected and ensure that the name and FIN / SAP number is correct before sending. This is of particular significance given that approved external parties (e.g., councils, Multi-Agency Safeguarding Hubs (MASH) services) and other forces will have member access to certain Microsoft Teams, the likelihood of having multiple incidences of the same / similar name will be higher. Please be vigilant regarding external members of a Team when sharing documentation meant for internal use only.

2.5 Under no circumstances must Teams Chat be sent from an account that the user does not have the authority to send from as this is an offence under the Computer Misuse Act 1990.

2.6 Users are personally liable for all messages sent from their Teams Chat.

2.7 You must remain aware of who is around you at all times to avoid any unauthorised viewing or access to your Microsoft Teams Chat.

2.8 Teams Chat is subject to a deletion policy, in line with email, of two years. This means that content over two years old will be automatically deleted.

3. Unacceptable Use of Instant Messaging via Teams Chat

3.1 The Force will not tolerate any abusive, offensive, sexually explicit, or discriminatory instant messaging using the written word, GIFS, emojis, stickers or Avatars. The following list (not exhaustive) details what is unacceptable use of Teams Chat and expressly prohibited:

- To attempt to circumvent or to circumvent any security or restrictive features of Teams Chat or to expose it to unwarranted risks to confidentiality, availability or integrity through use that contravenes this procedure.
- Unauthorised use of a Microsoft Teams Account or other users accounts.
- To permit, grant or use the Teams Chat of another user, or to allow persons outside of Surrey Police and Sussex Police to do so, without authorisation from the Head of Technology and Data. This also includes, but is not limited to, users whose access has been denied or terminated.
- Sending or copying unauthorised messages that disclose personal information. This shall also include accessing, transmitting or seeking confidential / sensitive information about stakeholders or other users, unless it can be justified by operational needs or legitimate requests under the [Data Protection Act 2018](#), [UK General Data Protection Regulations \(UK GDPR\)](#) or [Freedom of Information Act 2000](#) legislation.
- Participating in activities, including the preparation or dissemination of content, which could damage the reputation and integrity of Surrey Police and/or Sussex Police.
- Any form of harassment, whether through language, image, frequency, or size of messages.
- The creation or distribution of, or engaging in, any disruptive or unethical activities, offensive or inappropriate messages, relating to comments, specifically, but without limitation to material about sexual activity, race, gender, disabilities, age, sexual orientation, pornography, religious beliefs and practice, or national origin, or any material that can be construed as offensive.
- Gambling in any form.
- Engaging in any criminal activity.
- Distributing copyright materials, for example, software, articles, music, video, and graphics, protected by copyright, unless required for police business purposes, for example, investigating an allegation of crime.
- Operating a business, soliciting money for personal gain, or otherwise engaging in any commercial activity outside the scope of employment, even where a “business interest” has been registered with Professional Standards Department (PSD).

- Sending or forwarding any jokes and/or attachments (for example, video clips or cartoons) that contravene this procedure or where this could cause offence to the recipient(s).
- Teams Chat should not be used for covert operations where alternative policing software is available which provides the anonymity and security measures to protect serving officers and staff.
- Additionally, Teams Chat should not be used to discuss covert policing tactics, methodology or activity or anything else that could present an operational security breach should it be revealed.

4. Privacy and Monitoring

4.1 All Force Teams Chat conversations are subject to audit logging and potential manual monitoring, scrutiny, or intervention by the Digital, Data and Technology Department (DDaT) or PSD.

4.2 Surrey Police, Sussex Police and the Police and Crime Commissioners (PCC) reserve the right to:

- Audit networks and systems on a periodic basis to ensure compliance with this procedure.
- Access, read, review, monitor and/or copy all messages and files on its computer systems at any time and without notice, unless exempted by this procedure.
- Disclose text, image, or sound files to other law enforcement agencies without the consent of the author or recipient concerned, if deemed necessary.

4.3 It is not possible for users to export entire Teams Chat for disclosure purposes. Action is currently limited to copy and paste and single-entry export to Outlook. Should a conversation history be required, the user will need to contact DDaT and Information Security to manage the extraction along with a justification.

4.4 Quarterly audit of Teams permissions changes including joiners, movers and leavers to be completed and document any changes of site owners.

5. Protective Marking

5.1 No material above OFFICIAL with a handling caveat of SENSITIVE should be transmitted over Microsoft Teams (including Teams Chat) in any format.

5.2 Sensitivity labels cannot be applied within a Teams Chat, therefore these should be applied to a document prior to sharing, when open in One Drive App, SharePoint App or via Office.com. Guidance on how to apply sensitivity labels can be found here: [Managing your information in the Cloud \(sharepoint.com\)](https://sharepoint.com).

5.3 For further information, please see the Surrey Police and Sussex Police Information Security Policy (722) Government Security Classification Procedure.

6. Remote Working

6.1 The same care should be taken using all functions of Microsoft Teams outside of a secure police location as users would with any other typed or verbal correspondence. Please be aware of your surroundings at all times, including what could be overheard or seen by those in your vicinity or other participants on the audio / video call.

6.2 Refer to the Surrey Police and Sussex Police Information Security Policy (722) Remote and Home Working Procedure for further guidance.

7. Support for Users

7.1 For support refer to Microsoft 365 Learning Hub and choose Microsoft Teams.

8. Security Incidents

8.1 In accordance with the Forces Security Incident Reporting Procedure (refer to the Surrey Police and Sussex Police Information Security Policy (722)), users must report any security incidents, malfunctions or suspected security weakness to the IT Service desk and Security and Information Assurance Team via the Security and Breach Reporting Tool found on the front page of the intranet.

8.2 Individuals receiving inappropriate messages via Teams Chat messages from any source are required to report the matter to their line management in the first instance, unless there is a compelling reason for not doing so. If this is not possible or appropriate, then this can be reported to PSD or via the Anonymous system (Surrey) / Break the Silence (Sussex). Failure to report as soon as practicable may be considered a breach of the Code of Ethics and lead to an investigation.

9. Security of Messages in the Cloud

9.1 Traffic through the Microsoft Cloud and the Force tenant is monitored nationally via the National Monitoring Centre for policing, and in-built security protocols in adherence to national guidelines.

9.2 All traffic is logged for security monitoring purposes, and the logs include details of the flow of information but not the content.

10. Roles and Responsibilities

10.1 The decision to send a Teams Chat and responsibility for the content of that message rests with the sender. Users are accountable for their use of the Force's information systems.

10.2 Disciplinary action may be taken against the sender of a Teams Chat with content that is seen as libellous, pornographic, sexist, racist, malicious, harassing in nature etc. or is likely to cause offence or distress to an individual or business.

10.3 The Forces may monitor, and access individual and group Teams Chats in the course of an investigation, in line with lawful business monitoring when a legal basis is established.

Team: Security and Information Assurance