



Force Skype for Business Systems (Surrey and Sussex) (1200/2024)

Abstract

This policy and associated procedure apply to all users entitled to access and use the Force Skype for Business System.

Policy

1. Introduction

1.1 This policy and associated procedure apply to all users entitled to access and use the Force Skype for Business System. Skype for Business is a unified communications (UC) platform that allows text based, video / voice-based communications, screen sharing, voicemail, file transfer and integration with email utilising the existing data network. Access to and use of the Force Skype for Business System will only be granted once vetting has been completed and a Force account has been issued. Microsoft Teams has now also been introduced to the Forces for meetings, messaging, and calls. Teams should be the primary tool used for communication where possible.

2. Scope

2.1 This policy and procedure cover all information conveyed over the Force Skype for Business System and it is the responsibility of every Force Skype for Business Systems user to know this procedure and to conduct their activities accordingly.

3. Policy Statement

3.1 The Force Skype for Business System is to be used to communicate with colleagues within Surrey Police and Sussex Police also to access externally hosted meetings.

Procedure

1. Definitions

- 1.1 • Instant Text Communication - one on one text communication between users.
- Presence States - a combination of colour indicator and text string to indicate users' availability.
- Document Sharing - the ability to send a document for collaborative working.
- Desktop Sharing - the ability to show another user your screen content as you see it.
- Voice Calling - one on one voice communication between users.
- Video Calling - one on one visual communication between users.

- Multi-party Conversation / Conference - the ability to hold a multi-person voice or visual communication session.
- Telephony - the ability for users to make and receive telephone calls with internal and external participants from the Force Skype for Business System. This has replaced the use of legacy desk phones which in some areas of the business are being replaced with Skype compatible desk phones. This is a joint Forces voice solution.
- Externally Hosted Meetings - users can join Skype for Business meetings which are being hosted by our external partners but should seek advice from Security and Information Assurance to ensure appropriate controls are in place.

2. Privacy and Monitoring

2.1 All Force Skype for Business System communications may be subject of audit and monitoring by the Professional Standards Department (PSD) and Digital, Data and Technology Department (DDAT).

2.2 Surrey Police, Sussex Police and the Police and Crime Commissioner (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.

3. Acceptable Use

3.1 The Force Skype for Business System is for police business use. Limited personal use may be permitted. Refer to the Use of Email Procedure within the Surrey Police and Sussex Police Information Security Policy (722) for further information.

3.2 Any Force Skype for Business System 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 the Skype for Business system. Only use text that you could personally justify, for example, if read out in court.

3.3 Users should regularly check their Force Skype for Business System account for new messages and maintain their availability status.

4. Unacceptable Use

4.1 The Forces will not tolerate any abusive, offensive, sexually explicit, or discriminatory e-mails messages (textual video or audio). The following list (not exhaustive) details what is unacceptable use of the Force Skype for Business System and expressly prohibited.

- To attempt to circumvent or to circumvent any security or restrictive features of the Skype for Business System or to expose the Force Skype for Business System to

unwarranted risks to confidentiality, availability or integrity through use that contravenes this procedure.

- Unauthorised use of the Force Skype for Business System or other users accounts.
- To permit, grant or use the Force Skype for Business System account of another user, or to allow persons outside of Surrey Police and Sussex Police to do so, without authorisation from the Head of Strategic Systems. This also includes, but is not limited to, users whose access has been denied or terminated.
- Sending or forwarding 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 UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018 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 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 PSD.
- Creating or forwarding chain letters or ‘pyramid’ schemes of any type.
- 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).
- Storing, receiving, sending, or forwarding personal scanned or digital photographs or images copied or downloaded from the Internet of any type (for example, video or still images) or any format (for example, jpeg, bitmaps) or could breach copyright legislation are not permitted, unless for authorised or specific police purposes.
- Additional personal Force Skype for Business System accounts are not permitted.

5. Protective Marking

5.1 No material above OFFICIAL should be transmitted over the Force Skype for Business System in any format. For more detail, please see the Government Security Classification Guidance within the Surrey Police and Sussex Police Information Security Policy (722).

6. Remote Working

6.1 The same care should be taken using all functions of the Force Skype for Business System 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, refer to the Remote and Home Working Procedure within the Surrey Police and Sussex Police Information Security Policy (722) for further guidance.

7. Support for Users

7.1 It is expected that the Forces will provide support to users to ensure that the appropriate tools are available to enable colleagues to complete their role. A Skype for Business User Guide has been produced which provides step-by-step instructions and screenshots of basic functionality.

If further support or specialist equipment (i.e., a mono headset which does not interfere with a hearing aid) is required this should be managed via the line manager in the first instance who can arrange Occupational Health and Access to Work referrals.

Consideration should be given to users involved in calls or conferences who may be neurodivergent or have learning differences. It may be necessary for meeting chairs to consider how the meeting is structured and what is expected of users on the call. For example, whether attendees are comfortable having their cameras on and the potential for visual stress / sensory overload that could create. Whilst Skype allows these functions to be used during calls and conferences, it will need to be at the discretion of those involved as to which are enabled.

8. Security Incidents

8.1 In accordance with the Force Security Incident Reporting Procedure, users must report any security incidents, malfunctions or suspected security weakness to the IT Service desk and the Security and Breach Reporting Tool found on the front page of the intranet.

9. Virus and/or other Warnings and IT Systems Messages

9.1 Do not forward these warnings to other users, as these messages are often disruptive hoaxes. Any user, who suspects a virus, should stop using the system and contact the IT Service Desk immediately.

9.2 Individuals receiving inappropriate messages via the Force Skype for Business System 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. Failure to report as soon as practicable may be considered a breach of the Code of Ethics and lead to investigation.

10. Screen sharing

10.1 Users should be aware that if you have shared your screen during a Force Skype for Business System call / conference, that the other users within this call will continue to see your screen until you select the option to stop screen sharing or close the call window entirely. Ending the call itself does not prevent users being able to see your screen and could lead to information being unintentionally visible.

Team: Security and Information Assurance