Reference for Data Privacy Impact Assessment

Contents

Version Control

	Date	Author	Notes
1.	2020-12-08	Tim Verlander	
2.	2020-12-16	Lynne Taylor	
3.	2021-02-01	Tim Verlander	Accuracy check, minor supplier changes
4.	2021-04-15	Tim Verlander	Update for public launch
5.	2024-04-16	Toni Denton	Update to new template, accuracy check

Reference for DPIA

This document provides guidance of how teamSOS acts as a data processor of the organisational data supplied by a customer. It details how the rights and freedoms of the data subjects are met and how risks may be reduced.

It is the responsibility of the Data Controller the undertake a DPIA of any system they operate in their organisation. However, teamSOS provides this reference DPIA to assist in this process.

While this document is largely general to all use cases for teamSOS, in certain sections it refers specifically to use in an education setting for best overall context.

What does teamSOS do?

teamSOS is the simple incident response system that puts schools and trusts on the front-foot, linking together the right people and guidance to resolve every type of incident quickly and effectively. It provides rapid alerts when staff need help giving the User a one-click option to alert responders for critical incidents.

There is a live-stream facility within the teamSOS app to send live video of an incident scene to the wider response team. With its announcements feature the app expediates schools' "lockdown" and "evacuation" alerts to ensure the whole school is informed and knows how to respond. The app employs a smart GPS system which can pinpoint the location where the incident is happening.

Who is the Data Controller and who is the Data Processor?

The customer organisation is the Data Controller.

teamSOS is a Data Processor and acts under instruction of the Data Controller.

teamSOS uses additional services, such as cloud hosting, provided by third parties. Third party suppliers that handle personal data are outlined in: **Appendix 3: Sub-Processors to teamSOS and are subject to change.**

Defining Data Subjects in teamSOS

teamSOS defines two sets of data subjects within the product and platform. The processing of data, and hence the data privacy impact is different for these two sets of data subjects.

User Subjects

Commonly an organisation employee. These data subjects are authorised users who can access teamSOS for their workplace purposes, are imported into teamSOS by the organisation administrator, and whose user accounts are controlled by the organisation administrator. The credentials of a user subject may be verified via single sign-on.

Content Subjects

The subject(s) of an Incident or a Chat group. These data subjects are within the responsibility and legal processing scope of the organisation and may or may not also be a User Subject. For example:

- A disruptive student who is named in an Incident requesting their removal from class
- A group of three students on a school trip who have gone missing
- An injured colleague who is the subject of an incident
- An external contractor to the organisation who is discussed by two User Subjects in a chat message
- A student who is captured shouting in the background of an audio LiveStream during an incident

In all cases, a Content Subject is expected to be a data subject that has a legal relationship with the organisation.

Responses to DPIA Screening Questions

This section answers the typical questions that an organisation will ask before determining whether to undertake a DPIA.

Does this project involve processing personal data?

Yes, both for User Subjects and Content Subjects.

Please refer to Appendix 1: Data Items Processed by teamSOS for specific details.

Is the project new to the school and involves the processing of information about individuals, or an existing system which collects new information, or has a change in purpose, or processes data deemed to be at risk?

Details Yes, both for User Subjects and Content Subjects

For User Subjects this includes the following categories:

- Staff user profile data, such as name, email address, avatar icon
- Location data, when a staff user is conversing in an incident or emergency and not in the background
- Technical operation data, such as cookies, tokens, hashed passwords, device identifiers and so on

For Content Subjects this includes the following categories:

- Content data, which may contain written, audio or photo details of students or other personal content
- Special category data, about a specific data subject as necessarily disclosed to a closed response group during an incident or emergency

Further detail and definition of these categories is detailed in Appendix 1: Data Items Processed by teamSOS

Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?

No.

teamSOS operates role-based access control for specific authenticated and authorised users as permitted by the Data Controller and does not transfer personal data outside of the organisational boundary.

Further, within teamSOS the membership of any SOS Emergency or Incident response team is also controlled by the Data Controller. Whilst during an emergency or an extraordinary event there are people or organisations who will need to be given access to information who would not normally need it. However, these people would require this information no matter what system or process is used during an emergency.

Does the project involve using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition?

Yes.

teamSOS uses existing and well-established technologies to replace legacy technologies or manual processes with streamlined and audited equivalents.

However, the teamSOS app will optionally record and share the location of a User Subject when they create an Incident. This also happens for any other persons responding to the Incident. This is to facilitate fast and effective response but may be considered a use of new technology. We do not track location on an ongoing basis, and thus believe that the balance of privacy in the interests of the individual is preserved.

teamSOS may also undertake speech recognition activities, for example in transcribing push-to-talk messages sent by User Subjects during an incident or chat to facilitate more efficient communications. Personal data generated by any such activities remains fully within the scope of the Data Controller.

With any modernisation process the Data Controller should be aware of potential risks in their own environment, please refer to Appendix 2: Assessing Privacy Risks with teamSOS for guidance on this.

Will the project result in making decisions or taking action against individuals in ways that can have significant impact on them?

No.

teamSOS supports and enables existing processes, including improvement of adherence to process and access to relevant information, but does not itself introduce new decisions or actions. teamSOS provides additional audit and due diligence information and improves the tools used to respond to minor or major incidents.

teamSOS does not adjust existing organisational decision processes and does not undertake any automated profiling or AI-based decision making. It gives users more timely access to information that would otherwise be gathered informally but the scope and process are unchanged.

Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records, or other information that people would consider to be private.

Yes, this is possible for Content Subjects.

As an emergency incident system that captures evidence in real-time and provides the means to undertake post-incident audit and aid future process improvements, teamSOS may be used to store information about at-risk students, those with behavioural issues, and/or real-time audio streams from a serious incident.

The data items are detailed in Appendix 1: Data Items Processed by teamSOS, and the later section of this document Identifying, Assessing and Mitigating Risks reviews the risks and mitigations.

What is the Lawful basis of processing? It is essential to establish that there is a Lawful basis for processing any personal data, under Art.6 and Art. 9 (where appropriate). There may be more than one Lawful basis for processing. Select the most appropriate

It is the responsibility of the Data Controller to determine the Lawful basis of processing, the below provides a likely basis for an educational organisation in England or Wales.

The lawful basis of processing for teamSOS may use (Art 6.1(c)): “processing is necessary for compliance with a legal obligation to which the controller is subject;”

Alternatively, the lawful basis may be (Art 9.2(g)): “Processing is necessary for reasons of substantial public interest.” with the Condition being

12 – Regulatory requirement

18 – Safeguarding of children and individuals at risk

19 – Safeguarding of economic wellbeing of certain individuals

In England and Wales, the likely legal obligation for data subjects considered to be students is based in the DfE’s statutory guidance “Keeping children safe in education” which in turn is based on the following laws:

- Section 175 of the Education Act 2002,
- Education (Independent School Standards) Regulations 2014,
- Non-Maintained Special Schools (England) Regulations 2015,
- Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 (RIDDOR)

In England and Wales, the likely legal obligation for data subjects considered to be staff or visitors is based on:

- Health and Safety at Work Act 1974,
- Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 (RIDDOR)

Certain disclosures made during SOS Emergency incidents when using teamSOS may also be lawful under Vital Interests 6(1)d. An organisation should refer to their own existing guidance on such matters, regardless of which technologies (or absence of technologies) facilitate those disclosures.

To lawfully process special category data, you must identify both a lawful basis under Article 6 of the GDPR and a separate condition for processing under Article 9. Consent is sought by all schools to use student personal data throughout the curriculum and pastoral care. When seeking this consent, it should be made clear that special category data is included.

Would people expect their data to be processed in this way?

Yes.

The processing of this data is based upon legal obligations of the organisation as outlined in the previous question.

Would there be a significant impact on the individual because of processing?

Yes.

teamSOS supports and improves existing process but does it better and faster. In addition, teamSOS provides additional audit and due diligence information. It does not adjust existing organisational decision processes and does not undertake any automated profiling or AI-based decision making.

Does your organisation have a nominated Data Protection Officer?

No.

Our Data Protection Lead is reachable via dpl@teamsos.co.uk and is supported by our senior leadership team who are formally qualified in GDPR and well experienced in the practise of GDPR in the UK education sector.

In line with ICO guidance1 a Data Protection Officer is required for public authorities or bodies, or where an organisations core activities require the large scale, regular and systematic monitoring of individuals, or where an organisations core activities require the large scale processing of special category data or data relating to criminal convictions and offences.

At the time of writing teamSOS does not meet the criteria for mandatory appointment of a Data Protection Officer, and as such our assignment of a Data Protection Lead along with our robust process and policies, outlined in this document, sufficiently meets our responsibility to protect personal data. We continue review this assessment on a quarterly basis.

Identifying the need for a DPIA

Only the Data Controller can make the assertion whether an organisation needs to undertake a DPIA to use teamSOS, and for what reasons the organisation does or does not determine a DPIA is necessary.

This document aims to provide sufficient information to facilitate professional and full undertaking of a DPIA by the Data Controller. Please contact teamSOS if any further information is required to undertake a DPIA that this document does not already provide.

Common Use Cases and Data Privacy Risks

This section outlines common teamSOS use cases and discusses the potential data privacy risks. The product features to help manage these risks are outlined later in this document.

Creation of an SOS Emergency Incident	
Why does the organisation expose themselves to risk in this procedure?	Responding to any emergency carries risk to the responder(s), to any others in the setting and to the organisation itself. Decisions taken in the heat of the moment without time for detailed consideration can have grave consequences and may need to be defended later.
Is there any legal reason this must happen?	Any organisation has a duty to protect its workforce and visitors, and an educational organisation also has a duty of care to students. The organisation is obliged to record evidence of certain emergencies and in some cases is also obliged to report specific details to statutory bodies.
What else?	The organisation may also retain evidence in the event of potential investigation or legal action following a serious incident or SOS Emergency. By formalising emergency response in an audited and exportable manner the organisation builds a due diligence defence regarding their approach to serious incidents or SOS Emergencies. Such information then supports retrospectives to continually learn from incidents and improve procedures in the future.
What types of processing have been identified as likely high risk?	Per Appendix 1: Data Items Processed by teamSOS, the nature of any messaging, photo or audio content has a rare but present chance of containing Special Category Data. For example, in referencing the religion of a Content Subject in the scope of what medical interventions may or may not be permitted under their faith.

Are there any other risks?	As with use of any other digital communication technology in an educational setting, there is the risk of unintended disclosure by means of screen sharing, unlocked devices, broadcast audio, compromised credentials, etc.

Creation of a Routine Incident	
Why does the organisation expose themselves to risk in this procedure?	The organisation does not expose themselves to any new risk in this scenario, where, for example, a duty responder is requested to remove a disruptive student from a class.
Is there any legal reason this must happen?	Any organisation has a duty to protect its workforce and visitors, and an educational organisation also has a duty of care to students. The organisation may be obliged to record evidence of certain ongoing or developing behavioural issues to support a wider safeguarding duty.
What else?	The organisation may also retain evidence in case of potential investigation or legal action regarding an ongoing or developing behavioural issue. By formalising incident management in an audited and exportable manner the organisation builds a due diligence defence regarding their handling of the matter. Such information then also Page 9 supports retrospectives to continually learn and improve procedures in the future.
What types of processing have been identified as likely high risk?	No high-risk processing identified here.
Are there any other risks?	As with use of any other digital communication technology in an educational setting, there is the risk of unintended disclosure by means of screen sharing, unlocked devices, broadcast audio, compromised credentials, etc.

Creation of a peer-based Chat between Users	
Why does the organisation expose themselves to risk in this procedure?	The only risk is the retention of statements made by Users, which is the same whether via radio system, in person conversation, or other unmanaged instant messaging services such as WhatsApp and others.
Is there any legal reason this must happen?	We are not aware of any legal requirement to provide peer-based messaging tools to employees. However, the organisation has a legal responsibility to manage and protect its internal data and not take unnecessary risks; providing peer-based messaging affords an organisation greater control of the Content Data in those messages.
What else?	The use of a managed chat solution, rather than a third-party solution where each user controls data directly (such as WhatsApp and others) reduces the unintended disclosure risks for the organisation because the data is controlled by the Data Controller rather than by individuals.
What types of processing have been identified as likely high risk?	No high-risk processing identified here.
Are there any other risks?	As with use of any other digital communication technology in an educational setting, there is the risk of unintended disclosure by means of screen sharing, unlocked devices, broadcast audio, compromised credentials, etc.

The Scope of Data Processed

What is the nature of the data, and does it include special category or criminal offence data?

Appendix 1: Data Items Processed by teamSOS details the nature of data. This may include Special Category data about specific at-risk individuals as part of a professional and audited organisational response to an incident.

How much data does teamSOS collect and use?

The purpose of teamSOS implies that all teaching and administration staff in an organisation will be User Subjects.

No Special Category data is captured, processed, or required for User Subjects.

An incident in the school may include one or more students or staff as Content Subjects in the resulting conversation and processes that address the incident. A User Subject who is the focus of a specific emergency incident is therefore also a Content Subject during the lifecycle of that incident.

Where is personal data located?

Data is stored in the multi-tenant teamSOS cloud hosting environment, operating in Microsoft Azure within the UK and Ireland.

Excepting avatars and login tokens, personal data viewed in the teamSOS app is in memory only and not cached onto the device.

How many individuals could be affected by an unintended disclosure or data breach?

In a typical education deployment, all staff and students should be considered as potentially in scope. However, unless an unintended disclosure applied to the entirety of an organisation's teamSOS data, it is highly likely that any unintended disclosure would affect a far smaller number of User Subjects and Content Subjects. We provide measures such as role based access control and per-incident membership assignments to minimise risk and impact.

What geographical area does teamSOS process data within?

The teamSOS product and platform processes all personal data within the UK and Ireland. This does not prevent product access from overseas if an organisation deems it necessary, for example an educational trip.

The Purpose of Processing

What does your organisation intend to achieve by processing?

- Standardise the way we respond to SOS Emergencies and Incidents
- Reduce overheads and risks in getting help in the classroom or elsewhere on- or off-premises
- Get help faster through use of location responses, and provide interim information while help is on the way
- Ensure that staff have immediate access to the latest process steps for a range of Incidents
- Capture an exportable audit trail for SOS Emergencies and Incidents regardless of location or hybrid working
- Improve our overall ability to fulfil our legal obligations to students, employees, and visitors
- Reduce our compliance risks and exposure and increase our ability to make a due diligence defence

What is the intended effect on individuals?

- Improve our overall ability to fulfil our legal obligations to students, employees, and visitors
- Increase staff confidence by enabling them to access the most recent procedures and steps
- Enable staff to discretely obtain help without needing to send colleagues out of the classroom

What are the benefits of the processing for your organisation, and more broadly?

- Standardised SOS Emergency and Incident response whether on- or off-premises
- Free staff time, reduce administrative burden, and reduce dependency on legacy systems such as radios
- Improve the security of communications regarding Content Subjects
- Improve data control position by retreating from “personal” messaging services like WhatsApp and others
- Immutable history of serious emergencies and minor incidents for export and audit
- Enable simpler post-incident review and ongoing process improvement


teamSOS

Individual Data Subjects and the Operating Context

What is the nature of the relationship with the individual data subjects?

The organisation has a duty of care towards students and is obliged to provide a safe environment for employees and visitors.

How much control will individual data subjects have?

If the organisation is relying on legal obligation as the lawful basis then data subjects and guardians are unlikely to be able to give informed and qualified consent. Individual data subjects can object to the processing, but the organisation may not be obligated to accommodate such requests due to the overriding legal obligation.

Do the individual data subjects include children or other vulnerable groups?

Yes. A significant proportion of the student population are children, and both students and vulnerable groups may become Content Subjects through SOS Emergency or Incident activities by the organisation.

Are there prior concerns over this type of processing or security flaws?

Any online platform involved in safeguarding and serious incidents must provide robust and reliable protections for personal data.

Is teamSOS a different way of working in any way? What is the current state of technology in this area?

Yes. teamSOS research indicates that incident management in education is typically co-ordinated without audit, using “personal” messaging tools such as WhatsApp or similar, or by sending support staff for help and reducing the number of responsible persons present at the very moment a serious incident occurs.

teamSOS provides the essential functionality to enable staff and organisations to respond to serious emergencies and minor incidents quickly and reliably, in a way where personal data is properly controlled, and subsequent audit or evidence export are straightforward.

Are there any current issues of public concern that should be factored in?

Yes. The increased frequency of serious and high-profile incidents in schools that risk the personal safety of students and staff alike is precisely why teamSOS has been designed. The ongoing requirement for staff and students in education to operate hybrid working and hybrid learning introduces new real time communication, audit, information management, and access challenges that teamSOS helps address

Compliance and Proportionality

Are there any other ways to achieve the same outcome?

teamSOS is unique in the features offered in an education setting. While organisations can make use of external “personal” messaging tools such as WhatsApp or similar, this doesn’t provide the same organisational control of Content Data and presents additional risks to Content Subjects. Other more manual processes can be employed, but not with the same benefits around evidencing compliance, export of historic incidents, or continual process improvement.

How will you prevent function creep and avoid use of technology beyond the originally intended purpose?

teamSOS is designed to help an organisation model their existing and new processes. Its purpose includes supporting staff in daily activities and ensuring that the most recent steps to take are available to staff and that responsibilities for specific actions are clearly delegated. Any further usage would require a re-assessment of an existing DPIA, especially in cases where new areas of data are introduced.

How will you ensure data quality and data minimisation?

teamSOS operates data minimisation across all platforms for User Subjects, and the specific purposes for each processed data item are outlined in: Appendix 1: Data Items Processed by teamSOS.

Content Data, referring to the occurrence and subsequent audit of any SOS Emergency or Incident is stored verbatim until exported and/or deleted by the organisation.

How are data subject rights supported?

Given the nature of the processing, Content Subjects have limited rights for erasure, objection, or restriction. User Subjects can have their personal data corrected at any time, either by direct action or by the organisation depending on the specific data item. Rectification can be undertaken to the extent that it doesn’t alter the recorded historic event of an SOS Emergency or Incident or that such rectification forms a post-event annotation to an SOS Emergency or

Incident. Access can be made by the organisation for SOS Emergencies and Incidents. Peer-based chat records can be retrieved by teamSOS support subject to appropriate instruction. Data Transfer is undertaken by support request.

Information is provided by Privacy Notice. There is no automated decision making.

What measures does teamSOS take to ensure their sub-processors are compliant?

teamSOS operates a data minimisation principle and avoids external sub-processors where practical. Where we do use sub-processors in our product platform, we ensure they are reputable and compliant with prevailing legislation.

Please see Appendix 3: Sub-Processors for more detail.

How does teamSOS safeguard international transfers?

There are no international transfers within the teamSOS platform, all data is processed within the UK and Ireland.

The use of the teamSOS App overseas is subject to organisation policy, which can freely include multi-factor authentication via single sign-on. The teamSOS App does not store personal data locally, except for user avatars and OAuth2 authentication tokens, and all transfers from teamSOS servers to and from the App are subject to TLS 1.2,OAuth2 scoped access controls, and role-based access controls.

Identifying, Assessing and Mitigating Risks

This section provides a summary risk analysis group by actor and is accompanied by a detailed risk assessment included in Appendix 2: Detailed Risk Assessment of teamSOS. Numbers in brackets below refer to specific assessed risks.

Actor: Cyber Criminals

Actors outside of your organisation that are deliberately attempting to cause damage or unintended disclosure.

Potential Risks

The risks presented by Cyber Criminals fall into two categories – unsophisticated attacks such as phishing attempts (1), snooping (2), and ransomware (3), and sophisticated attacks that are targeting at the teamSOS software directly (4, 5).

Probability of Occurrence and Severity of Harm

As there is limited financial value to the data contained in teamSOS the probability of attacks is lower than, for example, a school payments platform. However, any unintended disclosure of data could have a high level of harm for specific data subjects, particularly if the disclosure contained Special Category data or multiple Content Subjects.

Mitigations

teamSOS provides single sign-on and multi-factor authentication support. All data transfers are made using TLS 1.2 or higher. Personal data is not stored on client devices other than avatars and the current user OAuth2 authentication tokens. The teamSOS app stores authentication tokens using secure storage provided by theunderlying device operating system. The teamSOS cloud platform is architected from a security-first perspective and client accesses require access tokens, which themselves then restrict the scope of access for that user. Refresh tokens are restricted to single usage only.

Actor: Accidental Insiders

Actors within your organisation that may have a momentary lapse of judgement or make a mistake.

Potential Risks

The primary risk in this case, as with other school systems, is unintended disclosure of information that is accessible to the specific user. This could occur because of leaving a screen unlocked, not closing an app before using a Page 13 projector, or other similar accidents (6, 7). An unintended disclosure could also occur if users are not appropriately trained, or make a poor judgement, in disclosing sensitive information about a Content Subject – for example, their sexual life and orientation – in an inappropriate audience or when not required (8).

As with walkie talkies, for example, there is also the risk of unintended broadcast to those in the immediate surroundings when receiving a LiveStream or Push to Talk message (9). teamSOS provides mitigations for this.

Further lower risk scenarios relate to the loss or theft of devices (10) or inappropriate disposal of devices (11).

Probability of Occurrence and Severity of Harm

As with any communication tools the probability of occurrence depends highly upon the practices of the user. The severity of harm would vary depending on:

- the content and context of messages, Push to Talk, or LiveStream
- the amount of Content Data exposed
- the number of Content Subjects referenced and their vulnerability
- the size and makeup of the audience disclosed to

Mitigations

teamSOS will follow notification suppression settings at an OS level as configured in the OS per user, including suppression of notifications when Windows is remote screen sharing. The purpose of teamSOS is to provide an effective and audited communication system that provides an accurate historical representation of any incident affecting the organisation, therefore there is no manipulation or assessment of messages sent. The scope of any incident is, however, contained to a specific incident group which initially consists only of pre-defined responders and the requestor. As a result, any disclosure of e.g. Special Category data is likely to be within a suitable audience.

teamSOS makes the following mitigations to reduce the risk of an audio exposure:

- If the app is not currently open, then no audio is played back
- A Push to Talk message is only played back automatically if received while the app is open
- A SOS Emergency LiveStream is played back only if the user has opened the incident, and can be stopped
- The app uses the OS default sound output, for example if headphones are connected

The teamSOS app does not store personal data on client devices, other than avatars and the current user OAuth2 authentication tokens. The teamSOS app stores authentication tokens using secure storage provided by the underlying device operating system. Any existing user can be blocked using the teamSOS admin portal, preventing any further access to data.

Actor: Malicious Incidents

Actors within your organisation that intend to damage for personal gain or revenge.

Potential Risks

teamSOS uses group-based and role-based access controls to scope user access so the information accessible to a malicious insider will be limited to that range. However, as with any system used by the organisation, any Content Data within that range could be photographed by a malicious insider with the intent of unauthorised disclosure (12).

A user with administrative access to teamSOS could add new users to the platform or fail to delete leaver accounts (13), export Content Data (14), or delete SOS Emergencies or Incidents (15). As with any system used by any organisation, administrative access should be granted with consideration and reviewed on a regular basis.

Probability of Occurrence and Severity of Harm

Depending on the Content Data available to the malicious insider and the Content Subject(s) referenced, the impact could range from low to high.

Mitigations

teamSOS operates a pair development and code review model and maintains a Dev -> Test -> Live discipline via mature source control platforms. We have chosen Microsoft Azure cloud hosting as a secure and reliable platform to build upon. All teamSOS administrators are authenticated using Microsoft Azure AD single sign-on with multi-factor authentication. Access to underlying storage is limited to senior platform architects only and timeline message bodies are AES encrypted on a per-customer basis. teamSOS administrative user accounts are separate to daily-use teamSOS employee accounts.

Administrative access to teamSOS does not automatically permit access to customer data. To access customer data teamSOS must be granted support permission, which lasts for a fixed period before automatically revoking and therefore implementing automatic scope restriction to any compromised teamSOS administrator account.

Actor: Natural or Environmental Disasters

Pollution, flood, fire, wind, pandemic, and other uncontrollable external acts.

Potential Risks

As a cloud-based platform and distributed organisation, teamSOS presents minimal risks from physical disaster and could instead help in responding to it or operating in a heterogenous environment of on- and off-premises delivery. The most significant risk presented is reduced access for users caused by loss of connectivity or electricity (20), however we also consider the risk of a full cloud platform datacentre failure (21).

Probability of Occurrence and Severity of Harm

There is a minimal risk of harm because of natural or environmental disaster.

Mitigations

In the case of local issues, physical redundancy is the best option, and this cannot be implemented in software.

Examples would include additional mobile booster batteries and/or access to mobile data. A full cloud platform datacentre failure would affect a number of suppliers and realistically it is more likely that service would be restored by the provider before any disaster recovery to an alternative provider was fully undertaken.

Actor: Organisational Compliance

Failure by the organisation to comply with data protection legislation.

Potential Risks

When processing data by any means, including software products, the purpose of processing must be defined, data subjects must be appropriately notified, and risks adequately assessed. (22 - 27)

Probability of Occurrence and Severity of Harm

There is a low probability of compliance failure in UK education as the marketplace is aware of their obligations and, given the nature of data processed, takes them seriously. The severity of harm to individuals is also likely to be low as any adverse impact for compliance failure will affect the organisation itself.

Mitigations

This document provides detailed information to support enable an organisation to comply with data protection legislation when using teamSOS and is further supported by our privacy notice, service contracts, and other documentation. teamSOS are ready to assist with any further queries.

Appendix 1: Data Items Processed by teamSOS

User Subjects

teamSOS enables the creation of users for relevant organisational staff, who may then interact via the teamSOS App for daily use or via the web-based teamSOS Portal for administrative actions. The following data is processed:

User Profile Data	
Data Item	Purpose
Display Name	To provide context to new incidents, timeline messages, administrative actions, and response team membership. To enable conversation creation between colleagues.
Email Address	To provide a unique username for teamSOS To enable conversation creation between colleagues To follow up on tasks assigned to the data subject To facilitate single sign-on with existing organisational identity systems To enable self-service password reset
Avatar Image (which may be Display Name initials, an image uploaded to teamSOS, or an image they have uploaded to Office 365 or Google Workspace)	To provide quick recognition of context for new incidents and incident membership

Location Data	
Data Item	Purpose
Current Location (On demand, when interacting within an incident. There is no background tracking of location.)	To provide context of individual locations when responding to an incident, enabling faster attendance by colleagues. To provide context of individual locations when assessing the organisation response to a serious incident after the event

Technical Data	
Data Item	Purpose
Multi-factor authentication token (if enabled)	To increase the protections applied to the personal data stored within teamSOS that is accessible by the data subject.
A single sign-on token (Microsoft, Google)	To integrate with existing organisational identity lifecycle practices To increase the protections applied to the personal data stored within teamSOS that is accessible by the data subject To simplify and expedite access for an authorised data subject to teamSOS
One-way strong hashed password (When using single sign-on teamSOS does not store any password)	To facilitate secure access to teamSOS
Login session tokens	To facilitate secure access to teamSOS and enable revocation of existing access
Google reCAPTCHA cookie (when a data subject first logs in without using single sign-on or requests a forgotten password reset)	To increase the protections applied to the personal data stored within teamSOS that is accessible by the data subject
Device mobile push message token (when using the App)	To send relevant notifications to the teamSOS app when the app isn't open, such as new incidents, new instant messages, and so on
Device OS version installed (when using the App)	To ensure the technical format of notifications is suited to the capabilities of the OS and version

teamSOS app version installed (when using the App)	To ensure the technical format of notifications is suited to the capabilities of the app version installed
Unique installation identifier (when using the App)	To ensure that a given installation only receives notifications relevant to the currently logged in user
Diagnostic logs, not including timeline content (when submitting Feedback in the app and selecting to include logs)	To ensure that technical issues reported can be effectively investigated and resolved.

Content Subjects

teamSOS provides conversation features along with evidence capture and audit information in general use. The content is created by User Subjects but images and sound recordings, by their nature, may include other individuals present as deemed appropriate by the User Subject. Such information belongs to the Data Controller, is exportable for Incidents, and includes:

Content Data	
Data Item	Purpose
Incident messages (which contain any text typed by a user)	To enable audited exportable communication during an incident
Status messages (generated by teamSOS in response to user actions)	To provide audited exportable updates of developments as an incident unfolds
Push to Talk audio messages	To provide ad-hoc audited exportable communication during an incident in a manner faster than typed
LiveStream incident audio	To capture real-time audio evidence of an emergency incident and relay it to responders as it happens
Photo messages	To capture evidence of an incident and/or to provide additional context to responders
Peer-based chat messages	To enable communication between peers outside of an incident
Peer-based Push to Talk messages	To enable communication between peers outside of an incident
Peer-based Photo messages	To enable communication between peers outside of an incident

Special Category Data

Given the nature of the product it is possible for any Content Data to include disclosure of Sensitive Personal Data regarding the Content Subject in the context of the necessary conversation and within the judgement of the disclosing User Subject within that conversation, just as it is possible in all other content data produced by the organisation in all other forms and formats in any other product used.

For example, a message during an ongoing medical SOS Emergency may disclose the religion of a Content Subject in relation to the medical interventions that may or may not be acceptable to their faith.

Specifically, teamSOS assumes that Content Data could potentially contain any of the following:

- Medical records
- Ethnicity
- Religion
- Special educational needs

Appendix 2: Detailed Risk Assessment of teamSOS

This table details the risks identified in daily operation of teamSOS by an education organisation and their treated scoring. This information should be read in context of the supporting narrative in the section “Identifying, Assessing, and Mitigating Risks”.

Measuring average severity of harm:

- Low: A disclosure with typically minor personal impact for a low number of Data Subjects
- Moderate: A disclosure with typically minor personal impact for a high number of Data Subjects, or a disclosure
- with typically moderate personal impact for a low number of Data Subjects
- Severe: A disclosure with typically moderate or high personal impact for a high number of Data Subjects, or a
- disclosure with typically high personal impact for a low number of Data Subjects
- Transient: A period without access to data and not resulting in disclosure

Measuring overall risk score:

Severe	Medium	High	High
Moderate	Low	Medium	High
Low	Low	Low	Medium
Transient	Low	Low	Low
	Unlikely	**Possible**	**Possible**

No.	Describe the source of the risk and nature of potential impact on individuals. *Include associated compliance risks as necessary.*	Probability of Occurrence	Average Severity of Harm	Overall Risk Score	Risk Owner
1.	**Agent**: Cyber-criminal, malicious insider **Risk**: Account takeover **Vulnerability**: Poor account protection **Measures**: enforce use of strong user authentication (single sign on, multi factor authentication)	Unlikely	Moderate	Low	Customer
2.	**Agent**: Cyber-criminal, malicious insider **Risk**: Digital eavesdropping on digital communication, “shoulder surfing” **Vulnerability**: Poor physical security, lack of encryption **Measures**: Enforce use of encryption for data in transit. Improve premises to block view to unauthorised individuals	Unlikely	Low	Low	Customer
3.	**Agent**: Cyber criminal **Risk**: Ransomware attack **Vulnerability**: Poor endpoint protection, lack of security awareness training **Measures**: Improve technical endpoint protection, improve user training	Possible	Transient	Low	Customer
4.	**Agent**: Cyber-criminal, malicious insider **Risk**: Account theft **Vulnerability**: Authentication session token stored on accessing device **Measures**: Utilise OS-provided secure storage layers to offer maximum protection for session tokens	Unlikely	Moderate	Low	Joint
5.	**Agent**: Cyber-criminal, malicious insider **Risk**: Platform data storage compromise and/or unauthorised server-side code execution **Vulnerability**: Flaw in teamSOS cloud platform security, lost or stolen platform credentials **Measures**: Harden cloud platform security, protect or avoid credentials, use reputable cloud service providers	Unlikely	Severe	Medium	teamSOS

6.	**Agent**: Accidental insider **Risk**: Unintended passive information disclosure on an unlocked device **Vulnerability**: Poor data exfiltration control, lack of technical awareness, insufficient data leak prevention training **Measures**: Improve staff training, implement Data Leak Prevention training, configure notification suppression where supported by device OS when projecting or screen sharing.	Possible	Moderate	Medium	Customer
7.	**Agent**: Accidental insider **Risk**: Unintended passive information disclosure on a locked device **Vulnerability**: Poor physical protections for a locked device **Measures**: Improve staff training, implement Data Leak Prevention training, configure notification content suppression where supported by device OS when locked.	Possible	Low	Low	Joint
8.	**Agent**: Accidental insider **Risk**: Unintended active information disclosure to an inappropriate audience or containing unnecessary detail **Vulnerability**: Poor data exfiltration control, insufficient data protection training, lack of technical awareness **Measures**: Improve staff training, enforce use of encryption, Implement Data Leak Prevention	Possible	Moderate	Medium	Customer
9.	**Agent**: Accidental insider **Risk**: Unintended passive information disclosure via LiveStream audio or Push to Talk audio **Vulnerability**: Potential eavesdropping where audio is output from a device at a level where others can hear **Measures**: Improve staff training, implement Data Leak Prevention training, provide headsets or headphones to staff that are likely to be active audio users, mitigating product functionality	Possible	Low	Low	Customer

10.	**Agent**: Accidental Insider **Risk**: Loss or theft of device or media **Vulnerability**: Poor physical access control **Measures**: Enforce the use of encryption, enforce the use of remote device management policies	Possible	Low	Low	Joint
11.	**Agent**: Accidental insider **Risk**: Insecure device or media disposal **Vulnerability**: Lack of disposal facility, lack of education **Measures**: Staff training, set up secure disposal system, enforce use of remote device management policies	Possible	Low	Low	Customer
12.	**Agent**: Malicious insider **Risk**: Intentional duplication of personal data **Vulnerability**: Poor logical access control or management thereof **Measures**: Enforce governance practices for leavers, apply access control measures. If a malicious attacker is determined to act against the organisation there is little to done. However, have provisions in place to act swiftly to mitigate malpractices.	Possible	Severe	High	Customer
13.	**Agent**: Malicious insider **Risk**: Creation of unauthorised “sleeper” accounts or failure to close leaver accounts **Vulnerability**: Poor logical access control or management thereof **Measures**: Enforce governance practices for leavers, use single sign-on and multifactor authentication, ensure supervision and peer review of administrators. If a malicious attacker is determined to act against the organisation there is little to done. However, have provisions in place to act swiftly to mitigate malpractices.	Possible	Severe	High	Customer
14.	**Agent**: Malicious insider **Risk**: Unauthorised export of personal data **Vulnerability**: Poor logical access control or management thereof **Measures**: Ensure adequate practices for assignment and removal of administrative permissions. If a malicious attacker is determined to act against the organisation there is little to done. However, have provisions in place to act swiftly to mitigate malpractices.	Possible	Severe	High	Customer

15.	**Agent**: Malicious insider **Risk**: Malicious deletion of data **Vulnerability**: Poor logical access control or management thereof **Measures**: Ensure adequate practices for assignment and removal of administrative permissions, exports are retained by teamSOS platform for a period after SOS Emergency or Incident deletion	Possible	Transient	Low	Customer
16.	**Agent**: Data processor **Risk**: Unintended disclosure through mistake or software bug **Vulnerability**: Lack of due diligence on processor, lack of DP compliance by the processor **Measures**: Robust software development and testing processes, secure backups, pair working on significant technical issues	Possible	Moderate	Medium	teamSOS
17.	**Agent**: Data processor **Risk**: Unintended disclosure through cloud platform configuration fault **Vulnerability**: lack of redundancy, poor configuration management **Measures**: build for availability, secure backups, platform health and availability monitoring	Unlikely	Moderate	Low	teamSOS
18.	**Agent**: Data processor **Risk**: Unintended disclosure through lost or stolen user credential **Vulnerability**: poor credential management, lack of cyber security awareness **Measures**: restrict the scope of user access, automatically expire temporary access to customer data	Unlikely	Severe	Medium	teamSOS
19.	**Agent**: Data processor **Risk**: Unintended disclosure caused by human error **Vulnerability**: human process **Measures**: automate or codify where possible, data protection training, limit support access to personal data	Possible	Low	Low	teamSOS
20.	**Agent**: Environment **Risk**: Lost of access to product by a subset of users due to local environmental issues **Vulnerability**: Local electrical supply or Internet connectivity **Measures**: use of mobile devices, 4G	Possible	Transient	Low	Customer

21.	**Agent**: Environment **Risk**: Lost of access to product by all users due to environmental issues affecting cloud platforms **Vulnerability**: Local electrical supply or Internet connectivity **Measures**: remote secure backup, disaster recovery plan	Unlikely	Transient	Low	teamSOS
22.	**Agent**: Organisational compliance **Risk**: Failure to service Data Subject Request (Access, Erasure, Rectification, Restriction, Portability) in a timely or comprehensive fashion. **Vulnerability**: Lack of education, lack of cooperation or capability on the part of the processor, lack of trust from the data subjects. **Measures**: Raise staff awareness, improve training, suitable Data Processing Agreement in place	Possible	Transient	Medium	Customer
23.	**Agent**: Organisational compliance **Risk**: Lawful basis for processing not established or not sufficiently justified **Vulnerability**: Poor governance standards **Measures**: Staff training, undertake analysis of processing and determine the lawful basis.	Unlikely	Low	Low	Customer
24.	**Agent**: Organisational compliance **Risk**: Data protection principles violated: records not kept accurate **Vulnerability**: Lack of procedure **Measures**: Put in place policies, processes, and procedures so that data are kept accurate	Unlikely	Low	Low	Customer
25.	**Agent**: Organisational compliance **Risk**: Data protection principle violated: data erasure at end of useful life **Vulnerability**: Lack of procedure **Measures**: Put in place policies, processes, and procedures	Unlikely	Low	Low	Customer
26.	**Agent**: Organisational compliance **Risk**: Data subjects are not adequately informed of the data processing or the purpose is not suitably confined **Vulnerability**: Lack of education, Poor Governance **Measures**: Improve staff training and understanding, review, and publish privacy notice	Possible	Transient	Medium	Customer

Appendix 3: Sub-Processors to teamSOS

teamSOS engage the following sub-processors regarding personal data handling and are comfortable with these suppliers' ability to comply with relevant obligations.

Sub-Processor	Purpose
Microsoft Azure	teamSOS cloud platform hosting
Microsoft Office 365	Data management and communications
Apple APNS	Push notification to iOS authenticated mobile devices
Google Cloud & Firebase Cloud Messaging	Push notification to Android authenticated mobile devices
Microsoft WNS	Push notification to Windows authenticated devices
SendInBlue	Email communication to users
Google reCAPTCHA	Account protection when setting first-time password for user

Appendix 4: Example additions to school privacy notice

The example provided below may be used as-is or as the basis for any statement deemed necessary in the Privacy Notice advertised by a school customer.

"In compliance with our statutory obligation to provide a safe working environment for employees and visitors and to safeguard all students, we use incident management software to aid in the fast response and recording of SOS Emergencies and Incidents and to furnish our employees with the latest versions of our processes and policies. The historic record of any incident may include audio and visual assets as deemed appropriate at the time of the event. We act as Data Controller for these records and subject them to the same rigorous protections as all personal data in our care."