Great Ormond Street Hospital for Children
NHS Foundation Trust

Privacy & Security Impact Assessment

Title	Ref number
Microsoft Teams as a team communication app /knowledge base to help EPR Go-Live	PIA048

PAGE							
ISSUE							
DATE							

PRIVACY & SECURITY IMPACT ASSESSMENT

Introduction

A Privacy & Security Impact Assessment enables GOSH to meet its legal/compliance obligations with the Data Protection Act 2018.

The Privacy & Security Impact Assessment ensures the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to the Trust that risks are adequately managed.

It is important that the Privacy & Security Impact Assessment is part of and integrated with the organization's processes and overall management structure and that information security is considered in the design of processes, information systems, and controls.

The process identifies and allows issues to be mitigated at an early stage of implementation/change thereby reducing associated costs and damage to reputation.

Privacy & Security Impact Assessments are an integral part of the "privacy by design" approach. This approach has been identified by the Information Commissioner and its approach is legally required under the General Data Protection Regulations 2016.

Document Completion

A Privacy & Security Impact Assessment must be completed:

- where a **new** process or information asset is introduced that is likely to involve a new use of personal data or business critical information.
- where a **new** process or information asset is introduced that significantly changes the way in which personal data or business critical information is handled.
- where there is a change to an **existing** process or service that affects the way personal data or business critical information is handled.

This document, and the privacy risks, actions and recommendations identified within it, will be accepted in the Project Sign Off (page 3). The project will need to signed off by the implementer, a representative from Information Governance and a member of staff who has an appropriate level of responsibility for the project risks. Please note, sign off of this document does not close the privacy risks related to this project. It is important that the risks are revisited and any additional privacy risks identified are appropriately reviewed.

PLEASE NOTE:
The staff member (implementer) undertaking the Privacy & Security Impact Assessment has a responsibility to ensure that Patient Safety, Technical Security and Quality Impact Assessments are considered, in line with GOSH procedure.

PRIVACY & SECURITY IMPACT ASSESSMENT

Assessment Process Stages

Activity	Implementer	Information Governance
Complete Title Bar and include Ref Number	✓	
Complete Project Details and check the Initial Screening Questions	✓	
Complete Stage 1 – Introductory meeting and review Initial Screening Questions and follow up questions to determine if a Stage 2 – Privacy & Security Impact Assessment (Full) is to be undertaken	✓	✓
Initial Screening Questions to be formally written up and Introductory Meeting to be formally recorded		✓

If a Privacy & Security Impact Assessment (Full) **IS NOT** required		
Activity	**Implementer**	**Information Governance**
Complete Assessment Summary & Recommendations for Action		✓
Assessment to be passed to Implementer		✓
Ensure Sign Off is completed	✓	
Assessment to be kept with project documentation copy to Information Governance	✓	

OR

If a Privacy & Security Impact Assessment (Full) **IS** required		
Activity	**Implementer**	**Information Governance**
Complete Stage 2 – Privacy & Security Impact Assessment (Full)	✓	✓
Complete Stage – 3 Work Flow Mapping	✓	✓
Complete Stage – 4 Identified Risks and Mitigating Action	✓	✓
Complete Stage – 5 Legal Compliance		✓
Complete Assessment Summary & Recommendations for Action		✓
Closure meeting for final agreement	✓	✓
Ensure Sign Off is completed	✓	
Assessment to be kept with project documentation copy to Information Governance	✓	

PRIVACY & SECURITY IMPACT ASSESSMENT

Project Details

Project Title:	**Microsoft Teams as a team communication app /knowledge base to help EPR Go-Live**

Project Description:

Describe in sufficient detail for the proposal to be understood. Explain broadly what project aims to achieve and what type of processing it involves. It may be useful to consider any benefits of the project.

You may find it helpful to refer or link to other documents, such as a project proposal.

Team Communication at EPR Go-live 20.2.1

EPR programme – Improving Go-Live communication

Microsoft Teams as a team communication app /knowledge base to help EPR Go-Live

The Trust's implementation of the Electronic Patient Record (EPR) programme has looked to leverage the learning of other hospitals to enhance clinical system design, change management and support the successful enterprise wide implementation of Epic. We have taken proactive steps to avoid problems previously encountered by hospitals embarking on similar journeys.

The EPR programme represents the largest enterprise wide clinical transformation programme to affect GOSH in living memory. The Epic platform will replace at least 385 of 400 existing clinical systems. Whilst disparate, clunky and fragmented, these systems have been in place for many years allowing clinical staff to gain familiarity and allow often efficient working despite their individual failings. Nearly every clinical and operational task undertaken will have to be relearnt; new workflows, whilst often more efficient, will also require a learning curve until familiarisation and a working memory is learnt.

Why team communication and creation of a knowledge base is essential?

Go-live is a period defined as the point in which a hospital launches a new technology solution and prepares for issues, optimizes the system, brings the old system down and hopes that clinical staff adapts to the new technology. This is understandably a time of massive flux for the organisation, clinicians and patients and carries risk for the smooth running of the hospital.

A key learning from site-visits has been that Go-live success, in part, was attributed to the enterprise-wide use of a ***team*** **communication app** such as **WhatsApp** or **Slack** to enhance communication, between Core team members, super-users and external colleagues at this time and create a real-time knowledge base to fix EPR issues/tickets readily.

This approach significantly reduced the burden of IT help desk and allowed for the crowd-sourcing of knowledge directly back to users at a speed and scale previously unachievable. A clear message from Royal Children's Hospital, Melbourne and Sick Kids Hospital, Canada was that the use of a ***team*** **communication app** was not simply desirable but an essential tool at the time of Go-Live. The clinical utility of tools that provide team-based approaches to coordinating care is incredibly useful. The ability to self-organise and communicate as a team wherever you are, using your own phone, and to know when information has been received and read –are powerful and immediate benefits. The alternative, if the we dont step forward to use safer alternatives for clinicians / EPR Go-live is that WhatsApp's use will continue.

PRIVACY & SECURITY IMPACT ASSESSMENT

Context at GOSH / CCIO recommendation

The use of Microsoft Teams at GOSH confers huge clinical / operational and strategic advantage for our EPR Go-live. We have tried to best leverage the learning from other sites that have gone live with an enterprise wide installation of Epic. Most sites were heavily dependent upon **WhatsApp** during the Go-live window for extensive communication / messaging and escalation of information between staff (internal and external guests) themselves and Command.

Melbourne, intelligently used **Slack** - to add the additional layer of an integrated knowledge base (for super-users) to readily find fixes /solutions etc. This significantly improved their Go-live process and reduced ticket burden. This was a key learning from them.

We have looked at **Microsoft Teams** to provide a *team* **communication platform** and integrated knowledge base that is hosted by GOSH through Office 365.I have participated in an unscripted demo of the product first-hand and observed that native, 'vanilla' Teams is incredibly impressive and easy to use. I believe that it will significantly enhance our EPR Go-live. We have started a focussed trial of 12 users (prior to the further roll-out of 30 more users). **During this pilot test we have advised that we do not use patient identifiable data in the system.**

Team communication apps

WhatsApp is a consumer service that lacks built-in capabilities for employees to work together securely. Microsoft Teams is the hub for teamwork in Office 365 that integrates all the people, content, and tools your team needs to be more engaged and effective. When we use Office 365 to share information with co-workers and suppliers, we control our data. Microsoft does not mine our data for advertising purposes. Office 365 allows us to control data security.

Why Not WhatsApp? The downsides of WhatsApp for company employees:

- Insufficient data protection under European laws if the servers are located in the U.S.
- No backup of confidential, business content according to company policies
- No administration function for companies

- Lack of professional desktop or tablet clients
- No support for business file sharing solutions
- No integration in the companies' processes and IT systems
- No audit-proofing and no support for companies
- No protection against data loss
- Insufficient knowledge transfer within working groups,
- Inadequate backup procedures
- File upload limit 100 MB
- User identity has reduced viability unless their phone number is stored in your contacts/ self-registered
- WhatsApp's handing of groups is limited - when you are in the app you see the telephone numbers of all the people in the group and often also their names and telephone numbers (privacy issues)
- Limited to 256 users/ group
- Mixes your social and business group communications.

Why is Microsoft Teams better than WhatsApp?

- You do not need a SIM card to log in
- Provides similar functionality to Whatsapp with added safeguards - integrates with business workflow (via O365), staff can responds to message on any device, either cell , iPad, laptop or pc.
- Readily deployable.
- Focus on privacy and follows the latest GDPR rules
- Secure. Highly scalable.
- Can be personalised for Business use
- Clear identity of user / role in organisation (secondary impact on Trust of source comment / knowledge

- The app is business function orientated
- You can switch off notifications (supporting shift work)
- Receive messages when offline
- Has group video chat
- The app is business oriented
- Syncs to the cloud in a secure Azure Tenant under GOSH Control

Teams knowledge base

Knowledge can be readily shared evenly and quickly (very useful at Go-Live). Because change of membership has no impact on content availability. Newly added members have access to conversations and files accumulated from the start. You can set up 'Team channels' to suit the varying tasks or topics that come up and can provide relevant documents and helpful links within these channels in a clearly structured way

Summary and recommendations

Recommend the use of Microsoft Teams as a '*team* communication app' and 'knowledge base' to support our EPR go-live. This is a safer alternatives for clinicians and the Trust in place of Whatsapp.

Implementing Organisation:	Great Ormond Street Hospital NHS Trust

Staff involved in PIA assessment (Include Email Address):	[redacted]

Key Stakeholders: *Describe when and how you will seek*	[redacted]

individuals' views – or justify why it's not appropriate to do so.	GOSH Staff - Users

Additional Advice: *Please note, that if this project is in anyway novel, uses current state of technology or there are any current issues of public concern with regards to data collection and processing consulting information security experts, or any other experts be considered. Please ensure any consultation is documented.*	N/A

PRIVACY & SECURITY IMPACT ASSESSMENT

Project Sign Off

	Name	Job Title	Organisation	Date
Project Lead				?
Information Governance				?
Responsible Owner (IAO)				?
Data Protection Officer				

Assessment Summary

To be completed by Information Governance and Data Protection Officer:

Outcome of Privacy & Security Impact Assessment:	
1. Project/Implementation is recommended **NOT** to proceed, as significant risks have been identified.	□
2. Project/Implementation to proceed once identified risks have been mitigated as agreed.	□
3. Project/Implementation has met required legislative compliance and poses not significant risks. No further action required.	□

Summary of Privacy & Security Impact Assessment; including legislative compliance and identified risks:

Summary:

TEAMS deployment at GOSH (Issues – Clarification and Mitigations)

a) Microsoft's best practice recommendations for Azure and AD integration had previously not been met- this was discovered during this process. (Need to move from AD to AD Federated Services)

Mitigation - an external Microsoft partner (CDW) have been commissioned and is currently on-site to ensure this is resolved in the next week. This will allow us to move to an ADFS environment**.**

b) Lack of clarity as to what the system will be used for?

Mitigation – clarity - the system will be used for team communication to aid EPR go-live communication between the EPR team and super-users.

c) What information is expected to be shared? /Any privacy risks associated with the system and the mitigating solutions?

Mitigation – Sensitive Trust information including that of personal identifying health data nature will not be used.

Personal data for staff (names and job titles) may be used.

d) The service is live before IG sign-off?

Clarification - the service is currently in PILOT with 12 users and has NOT gone live. No PHI is stored or transmitted. Advice/ tip-sheets on how to use Epic have been shared. Sensitive Trust information including of a personally identifying nature will not be used.

f) Data residency

Mitigation Microsoft offers data residency to give enterprises control over where their global data is stored.

g) Subject Access request: Electronically Stored Information (ESI) relating to a patient should be readily indexable; concerns from legal departments arise around 1:1 chats as they create a greater legal exposure surface.

Mitigation as Teams will not be used to discuss patient care or have patient identifiable data at this time

h) App management control:

Mitigation -Microsoft has Teams admin settings that can be configured in the Office 365 admin centre that gives control over which external Apps are allowed restricting other app integration.

i). Permissions Model: Microsoft facilitates guest accounts for Microsoft Teams (essential for Go-Live communication with Epic / supporting clinicians (internal and external) These settings can be managed securely within Azure AD.

Mitigation – No business sensitive/ financial or PID is to be stored in Teams

j). Team and Channel creation and naming requires thought to avoid sprawl and duplication.

That is the mitigation

k). Hierarchical vs Flat Groups: The previous standard with email and DLs (distribution lists) has been to have hierarchical /nested groups. From a security perspective this allows for enterprise administration of access rights. In Teams, everything is flat: **Mitigation** clear communication to staff that document sharing is to be taken with caution at all times.

l. Exfiltration Risk: Microsoft Teams enables easy knowledge sharing through the use of voice, chat, and file sharing

Mitigated by not sharing PHI / business sensitive data.

Risks to GOSH:

Formal **information governance has not been formalised and signed off**

Clarification once this happens – it will be compliant with Trust Policies and the governments Minimum Cyber Security Standard

Risks to Data Subjects:

All risks have been mitigated. Sensitive Trust information including that of a personally identifying health data nature will not be used.

Recommendations for Action

Summary of Identified Recommendations:		
Recommendations:	**Recommendation Owner:**	**Agreed Deadline for action:**
Options to reduce or eliminate risk should be implemented as referenced at Stage 4 of this document. To be added as an Information Asset	[redacted]	**On Project sign off**

PRIVACY & SECURITY IMPACT ASSESSMENT

Stage 1 – Initial Screening Questions

Answering "**Yes**" to a screening questions below represents a potential IG risk factor that may have to be further analysed to ensure those risks are identified, assessed and fully mitigated. The decision to undertake a full PIA will be undertaken on a case by case basis by Corporate Governance.

Q	Screening question	Y/N	Justification for response
1	Will the project involve the collection of information about individuals?	N	
2	Will the project compel individuals to provide information about themselves?	N	
3	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	N	
4	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	N	
5	Are there processes in place to ensure data is relevant, accurate and up-to-date?	Y	Creation of an active knowledge base with administrators – highlighting the best response / removing incomplete posts
6	Are there security arrangements in place while the information is held?	Y	With Microsoft Teams, customers benefit from the Office 365 hyper-scale, enterprise-grade cloud. • Data encryption at all times, at-rest and in-transit. • GOSH data at rest remains in region • Ability to have local data residency for core customer data at rest, plus failover and disaster recovery (see data residency slide in the appendix for details) • Human back-up via on-call support engineers standing by 24×7 • Customer content is never accessible in logs or telemetry • Multi-factor authentication for enhanced identity protection. • Secure guest access with AAD managed guest accounts • Microsoft Teams supports key compliance standards including SOC 1, SOC 2, EU Model Clauses, HIPPA, GDPR, and more, and comes with built-in information protection including audit log search, eDiscovery and legal hold for channels, chats and files—and soon Data

PRIVACY & SECURITY IMPACT ASSESSMENT

Q	Screening question	Y/N	Justification for response
			Loss Prevention. • The Microsoft Teams admin center provides you with a single coherent admin experience where you can manage all aspects of Microsoft Teams including users, settings, and analytics. Teams provides enterprise manageability to configure and set policies at a per-user level and manage trusted apps for employees and the organization. • This also includes advanced call management controls include call routing, auto attendant, call queues, and reporting.
7	Does the project involve using new technology to the organisation?	Y	New but established enterprise software from Microsoft.
If you have answered "Yes" to any of the questions numbered 1-8 please proceed and complete stage 2.			
9	Is a Patient Safety Review required?	N	No patient identifying health data will not be used / stored.
10	Is a Quality Impact/Technical Security Review required?	Y	Currently being performed by CDW as part of move from AD to ADFS

Is a full Privacy Impact & Security Assessment required	
Y/N	Please justify response **Yes or No**
Y	New technology to the organisation. While the transfer of sensitive or personal data will not be advised over this system there is still the potential for this to happen.

PRIVACY & SECURITY IMPACT ASSESSMENT

Stage 2 – Privacy Impact & Security Assessment (Full)

Please answer the below questions in the boxes provided. To prevent duplication you may find it helpful to refer or link to other documents, such as project proposals or security documents.

If you have any queries with regards to any of the questions please contact he Information Governance Team.

2.1	What data will be collected?		
	Summarise the data that will be collected:		
	Microsoft Teams will be used to communicate and share knowledge with an initial focus on the EPR Go live period. Patient and confidential Trust data will not be shared over the application. Any data shared will be collected and stored		
	Personal Data: *Personal data is information that relates to an identified or identifiable individual.*		
	Identifiers (please specify) *This may include: name, identification number, location data; and an online identifier.*	The subject of the data collection *This may include: patients (please specify if this is a specific cohort of patients), families or relatives, staff; and members of the public.*	
	Work email address/name	Staff (or any invited external user)	
	Pseudonymised data (please specify) *Information which has had identifiers removed or replaced in order to pseudonymise the data is still personal data for the purposes of GDPR.*	n/a	
	Anonymised data (please specify) *Data is unlikely to be truly anonymous if users have access to other data which they could use to identify Data Subjects.*	n/a	
	Special categories of personal data:		
	Racial or ethnic origin		□
	Political opinions		□
	Religious or philosophical beliefs		□

	Trade union membership	□
	Genetic data	□
	Biometric data	□
	Health	□
	Sex life	□
	Sexual orientation	□
	Data about criminal convictions or offences	□
	Other data (please specify):	Any data shared through the application

2.2	Is the data being collected necessary to perform the specified task?	
	Y/N	Please justify response **Yes or No**
	Y	Data collected as part of the transfer of information (initially part of the operational delivery of EPR programme)

2.3	If personal data is processed, what is the purpose? These maps to a Lawful basis for processing the data under **Appendix A**. This is mandatory for any processing of personal data.		
	Purpose	Example	
	Direct care and Administrative Purposes	-Delivery of care -Sharing between individuals involved in care -Local clinical audit -Waiting list management - Performance against national targets	□
	Commissioning and planning purposes	-Legal requirements to provide data to health commissioners	□
	Research	-Studies with regards to patients with specific diagnosis	□
	Regulatory and public health functions	-Monitor health status to identify community health problems -Preparing for and responding to public health emergencies	□
	Safeguarding (following the provisions of the Children Acts 1989 and 2004, and the Care Act 2014)	-Safeguarding children and vulnerable adults -Sharing information for a safeguarding purpose (i.e. with social work)	□

	Employment	-Storing staff details -Contacting staff under employment laws	☒
	For any other purpose of processing personal data please contact the IG Manager to confirm the lawful basis for processing. This should be outlined below:		
	Purpose		
	Legal Basis for processing of personal data (Article 6, GDPR)		
	Legal Basis for processing of special categories of personal data (Article 9, GDPR)		
	Other:	Personal Data will not be shared with regards to patients, controlled by policy. Staff identifiers may be shared as required within their roles.	

2.4	Who are the Organisations or external individual involved in processing the data?	
	Organisations Name	Data Controller or Data Processor *The **Data Controller** is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.* *The **Data Processor**, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.*
	Individuals can be added to 'groups' or 'chats' temporarily	Personal data will not be shared over Teams. GOSH will be the owner of any data shared over Teams.

2.5	Will any information be held offsite or access given to any external parties?	
	Y/N	If **Yes**, an Information Sharing Protocol is required and outline document the controls. If data is stored in the Cloud please document the additional controls in place.
	Y	The data will be stored in an Office 356 Secure container within a GOSH controlled and secure Azure partition. The security elements of this have been set up and controlled by GOSH ICT.

2.6	Has a data flow mapping exercise been undertaken?	
	Y/N	If **Yes**, please provide a copy

		If **Yes** please provide a copy. If **No**, please outline the information flows.
	N	The only flows of information will between users and the Cloud to transfer messages. All transfers are encrypted.

2.7	What format is the data? *Please specify if this data will be electronic or paper and the data types* *e.g. text, images, video etc.*	
	Electronic data will be shared as text. Photos can be shared.	

2.8	Is there an ability to audit access to the information? And is there a plan/process of how to run and monitor this? *i.e. are we able to review access, actions and use of accounts*	
	Y/N	Please describe if answered **Yes.** If **NO** what contingencies are in place to prevent misuse?
	Y	Admin roles can audit the use of the system and messages sent for both Internal and Guest users. This will only be monitored initially when due to suspected misuse or on request.

2.9	Does the system involve new links with personal data held in other systems or have existing links been significantly changed?	
	Y/N	Please describe if answered **Yes**
	Y	A link with Active Directory (AD) for authentication of user access

2.10	How will the information be kept up to date and checked for accuracy and completeness? *e.g. demographic details will be checked against the SPINE, users be prompted to complete missing information*
	The system will be used for messaging – quality checks will be the users responsibility when messages are sent.

	Who will have access to the information? (list individuals or staff groups)		
	Data	Staff Group/Individual Role	Justification for access
	Access to the System	All GOSH staff with an AD	Requirement to message

		account	
	Full access to the information in the system	System Admins within ICT	Required to check user use is appropriate and for business continuity.
	Access to the System	External users	For communication with GOSH staff when invited through a secure link

2.12	How will access to the data be controlled? *Specify how changes in who should have access to the data will be administered* *e.g. linked to the Trust HR systems for leavers etc.*
	Staff access is linked to their Active Directory (windows log on). External users can be invited to the system and then removed after a certain time period. All guests in Teams are covered by the same compliance and auditing protection as the rest of Office 365, and guests can be managed securely within Azure AD.

2.13	Will data leave the Trust network?	
	Y/N	If **Yes**, outline how it will be secured.
	Y	The data will be encrypted when shared to user devices

2.14	What security measures have been implemented to secure access? *e.g. Username and Password, link to Active Directory, Secure Token access, Key locked filing cabinet etc.*
	Staff users linked to AD and its controls already implemented by GOSH. All guests in Teams are covered by the same compliance and auditing protection as the rest of Office 365, and guests can be managed securely within Azure AD.

2.15	What devices will be used to access the data and what controls have been implemented to secure these devices?	
	Devices *e.g. Trust computers, Any device with internet access*	Security *e.g. System access controls, device security requirements*

	Mobile devices only (Trust and personal)	No data is saved to the personal device/ or outside the application. Users will be given advice when they log in around the data to share.

2.16	Are disaster recovery and business contingency plans in place for the information?	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
	N	In the first instance this application is non-essential communication tool. The data will have Secure back-up in Secure Environment.

2.17	Has staff training been proposed or undertaken and did this include confidentiality and security topic areas?	
	Y/N	Please describe if answered **Yes**
	N	Intuitive Platform with user tip sheet provided reminding users of guidance. Staff will be guided by policy.

2.18	How will learning be supplemented and refreshed? *e.g. prompts at data entry, User guides, Standard Operating Procedures*
	A reminder of confidentiality will be displayed to users at log in. A user guide will be available to all staff. Email reminders will be sent to users. A screensaver will be set up

2.19	Will reports be produced or can personal/sensitive personal or business confidential information be extracted?	
	Y/N	Please describe if answered **Yes**
		Chats cannot be downloaded/saved to the devices Reports can be extracted by admin on request
	Who will be able to run reports/extract?	Only Admin roles

	Who will receive the reports and will they be published?	Ad Hoc, based on request
	What other controls will be in place?	Ad Hoc, based on request

2.20	Are plans in place for the **retention and destruction of the data**? *These should be in line with the Records Management Code of Practice for Health and Social Care 2016*	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
	Y	Data will be stored in the Cloud in line with GOSH retention requirements. Staff will not be able to delete data permanently.

2.21	If this new/revised function should stop, are there plans in place for how the information will be **retained / archived/ transferred or disposed of?**	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
	Y	GOSH is the owner of this data and Admins can extract it at any time.

2.22	Will individuals be informed about the proposed uses and share of their personal data?	
	Y/N	If **Yes**, please describe how. *e.g. updates to the Trust Privacy Notice, Information sheets provided or posters displayed etc.*
	N	
	If **No**, list the reason for not doing so *E.g. relying on an existing agreement, consent is implied, the project has s251 approval or other legal basis?*	
	The system will not be used to process personal data other than user identifiers when messages are sent. Users will have the ability to share personal data over the system but measures are taken to remind them not to. This is documented further in Stage 4 of this assessment – Identification of Risks and Mitigations.	

2.23	Are arrangements in place for recognising and responding to requests for access to data? *i.e. Requests for personal data under Data Protection Legislation or Requests for Corporate*

	data under Freedom of Information Legislation	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
	Y	Admin staff can report on system usage and extract data as required.

2.24	Have you considered the rights of the Data Subjects and how you will comply with these?	
	The GDPR provides the following rights for individuals:	How will you comply with these rights
	The right to be informed (Question 2.22) *Individuals have the right to be informed about the collection and use of their personal data*	The system will not be used for personal data other than user identifiers when messages are sent.
	The right of access (Question 2.23) *Individuals have the right to access their personal data*	The system will not be used for personal data. If there is suspected personal data within the system a search can be completed by the Admin.
	The right to rectification *The GDPR includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete.*	The system will not be used for personal data.
	The right to erasure *The GDPR introduces a right for individuals to have personal data erased.*	The system will not be used for personal data. If there is suspected personal data within the system a search can be completed by the Admin. Audits will be conducted on a regular basis to assess the appropriate use of the system
	The right to restrict processing *Individuals have the right to request the restriction or suppression of their personal data.*	The system will not be used for personal data.
	The right to data portability *The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.*	The system will not be used for personal data.
	The right to object *The GDPR gives individuals the*	The system will not be used for personal data.

	right to object to the processing of their personal data in certain circumstances.	
	Rights in relation to automated decision making and profiling.	The system will not be used for personal data.

2.25	Has an Information Asset Owner been assigned?	
	Y/N	Please provide contact name and job title if answered **Yes.** Please state why not if response is **No.**
	Y	[redacted]

2.26	Has this been registered as an Information Asset Register?	
	Y/N	If **Yes**, please provide the Information Asset Register reference number**.** If **No**, please state why.
	N	This will be registered before go live.

2.27	Has the impact to other GOSH systems/processes been considered and appropriate leads consulted and in particular technical security?	
	Y/N	Please describe if answered **Yes.** Please state what checks were undertaken if response is answered **No.**
	Y	ICT have been involved in the implementation and trial of this system.

Stage - 3 Information Flow Mapping

N/A

Stage - 4 Identified Risks and Mitigating Action

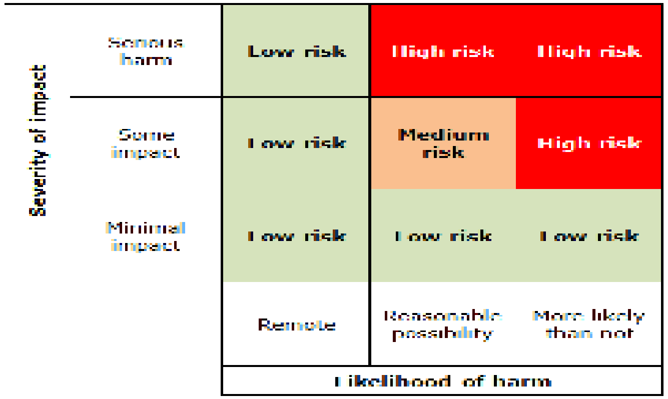
Use the provided table to document any privacy or information security risks identified from the above questions or additional risks that may exist. These could be to the Trust or data subjects. Examples may include inability to of individuals to exercise rights, illegitimate access or modification of personal data or loss of confidentiality. These risk should be scored using the Risk Assessment Matrix and for any risks considered 'High' or 'Medium' mitigating actions should be considered.

These may include:

- Deciding not to collect certain types of data
- Reducing the scope of the processing
- Taking additional technological security measures
- Training staff to ensure risks are anticipated and managed
- Anonymising or pseudonymising data where possible
- Writing internal guidance or processes to avoid risks
- Using a different technology
- Putting clear data sharing agreements into place
- Making changes to privacy notices
- Offering individuals the chance to opt out where appropriate
- Implementing new systems to help individuals to exercise their rights

When this table is completed it is important that any outstanding actions are assigned to an individual and documented. These actions could be incorporated back into an overall project plan.

Please note that any risks considered 'High' after mitigating actions have been applied should be alerted to the Information Governance Team as soon as identified.



Severity of impact	Serious harm	Low risk	High risk	High risk
	Some impact	Low risk	Medium risk	High risk
	Minimal impact	Low risk	Low risk	Low risk
		Remote	Reasonable possibility	More likely than not
		Likelihood of harm		

PRIVACY & SECURITY IMPACT ASSESSMENT

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary:	**Likelihood of harm** Remote, possible or probable	**Severity of harm** Minimal, significant or severe	**Overall risk** Low, medium or high	**Options to reduce or eliminate risk** Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk	**Effect on risk** Eliminated reduced accepted	**Residual risk** Low medium high	**Measure approved** Yes/no	**Mitigating Officer**	**Date to be completed:**
Personal patient information may be shared on the system. This could include photos.	Possible	Significant	Medium	-Reminders to be given to all users not to use the system of patient or sensitive information -User Guide clearly identifies this point -Audit plan for the system to assure the content is appropriate -Any reported breaches to be monitored (while this system will not remove this risk it will allow us more control and visibility over this sharing than external applications, such as Whats App)	Reduced	Low			
Individuals using their own devices for Trust work and Trust information saved or accessed on	Possible	Significant	Medium	As above	Reduced	Low			

unsecure devices									
GOSH data stored in the Cloud – to confirm security of the set up.				Steps taken to ensure security With Microsoft Teams, customers benefit from the Office 365 hyper-scale, enterprise-grade cloud. • Data encryption at all times, at-rest and in-transit. • GOSH data at rest remains in region • Ability to have local data residency for core customer data at rest, plus failover and disaster recovery (see data residency slide in the appendix for details) • Human back-up via on-call support engineers standing by 24×7 • Customer content is never accessible in logs or telemetry • Multi-factor authentication for enhanced identity protection. • Secure guest access with AAD managed guest accounts • Microsoft Teams					

				supports key compliance standards including SOC 1, SOC 2, EU Model Clauses, HIPPA, GDPR, and more, and comes with built-in information protection including audit log search, eDiscovery and legal hold for channels, chats and files—and soon Data Loss Prevention. • The Microsoft Teams admin center provides you with a single coherent admin experience where you can manage all aspects of Microsoft Teams including users, settings, and analytics. Teams provides enterprise manageability to configure and set policies at a per-user level and manage trusted apps for employees and the organization. • This also includes advanced call management controls include call routing, auto attendant, call queues, and reporting.					

				The setup has been reviewed by an external expert from CTW who has confirmed the current design set up is secure.					
While tightly monitored initially, after EPR go live function creep may lead to personal data being shared.	Probable	Significant	High	-Access and use of the system to be reviewed after EPR go live -Users to continue to be reminded of the use of the system -There is the potential for this to be used in the future to transfer sensitive personal and personal data, however if this is to happen this document will need to be reviewed and signed off. -If Microsoft 365 is adopted by the Trust Teams will form part of the project plan and roll out/review of this.					
External users can view GOSH messages	Possible	Significant	Medium	-Procedure to be put in place of any individuals external to GOSH who are given access- this includes when and how access is removed and any steps required before access is granted -Additional controls to ensure sensitive data					

				isn't shared on the platform					
Staff personal data will be shared in the form of the identifiers used (likely their name linked to email)	Remote	Minimal	Low	Risk considered low due to controlled access to the system. Staff names will already be accessible to anyone who has access to the global network. Security check of the Cloud environment removes the risk of unauthorised access to the data.					

*   Risk Assessment Matrix to be used

** if additional risks are identified please add to the notes section, Corp Governance will add on completion of form.

Appendix A

Purpose of using personal data	Examples	Conditions for lawful processing of personal data (Article 6 of GDPR)	Conditions for lawful processing special categories (including health) of personal data (Article 9 of GDPR)
Direct care and Administrative Purposes	-Delivery of care -Sharing between individuals involved in care -Local clinical audit -Waiting list management - Performance against national targets	6(1) (e) '…for the performance of a task carried out in the public interest or in the exercise of official authority…'	9(2) (h) '…medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems…'
Commissioning and planning purposes	-Legal requirements to provide data to health commissioners	6(1) (c) '…for compliance with a legal obligation…' or 6(1) (e) '…for the performance of a task carried out in the public interest or in the exercise of official authority…'	9(2) (h) '…medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems…'
Research (GOSH will still require consent or an appropriate legal basis (e.g. section 251 support) that meets confidentiality and ethical requirements to use personal identifiable data for research)	-Studies with regards to patients with specific diagnosis	6(1) (e) '…for the performance of a task carried out in the public interest or in the exercise of official authority…'	9(2)(j) '…scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or member State law which shall be proportionate…and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject …'
Regulatory and	-Monitor health	6(1) (c)	9(2)(I) '

public health functions	status to identify community health problems -Preparing for and responding to public health emergencies	‘…necessary for compliance with a legal obligation…’	…necessary for reasons of public interest in the area of public health…or ensuring high standards of quality and safety of health care and of medicinal products or medical devices…’
Safeguarding (following the provisions of the Children Acts 1989 and 2004, and the Care Act 2014)	-Safeguarding children and vulnerable adults -Sharing information for a safeguarding purpose (i.e. with social work)	6(1) (e) ‘…for the performance of a task carried out in the public interest or in the exercise of official authority…’	9(2)(b) ‘…is necessary for the purposes of carrying out the obligations and exercising the specific rights of the controller or of the data subject in the field of …social protection law in so far as it is authorised by Union or Member State law..’
Employment	-Storing staff details -Contacting staff under employment laws	6(1) (e) ‘…for the performance of a task carried out in the public interest or in the exercise of official authority…’	9(2)(b) ‘…is necessary for the purposes of carrying out the obligations and exercising the specific rights of the controller or of the data subject in the field of employment…social protection law in so far as it is authorised by Union or Member State law..’