Data Protection Impact Assessment: NHSmail live service with Office 365

Document Management

Revision History

Version	Date	Summary of Changes
0.4	February 2020	Uplifted to new DPIA template with JML and Exchange online additions
0.6	May 2020	Uplifted as per Steve Elgar Information Assurance review
0.7	May 2020	Uplifted as per IG SMT review
0.8	May 2020	Clean version reviewed and agreed by NHSmail
0.11	June 2020	Review by DPO and amended by NHSmail
1.0	June 2020	Version 1.0 finalised and published
1.1	June 2020	Final amends from DPO - finalised and published

Reviewers

This document must be reviewed by the following people:

Reviewer name	Title / Responsibility	Date	Version
Kieran Brough/ Clive Star	Technology Office	May 2020	1.1
John McGhie	Product Lead	June 2020	1.1
Mike Fisher	Senior Project Manager (JML)	June 2020	1.1
Office of the DPO	Office of the Data Protection Officer, NHS Digital	June 2020	1.1

Approved by

This document must be approved by the following people:

Name	Title / Responsibility	Date	Version
John McGhie	Product Lead	June 2020	1.1
Chris Parsons	Product Owner	June 2020	1.1

Glossary of Terms

Term / Abbreviation	What it stands for
MS	Microsoft
ESR	Link to Electronic Staff Record
NHSBSA	NHS Business Support Authority

Document Control:

The controlled copy of this document is maintained in the NHS Digital corporate network. Any copies of this document held outside of that area, in whatever format (e.g. paper, email attachment), are considered to have passed out of control and should be checked for currency and validity.

Contents

Purpose of this document

The purpose of this Data Protection Impact Assessment (DPIA) is to demonstrate how NHSmail complies with data protection laws in England for users of the NHSmail Live Service across Health & Social Care.

DPIAs are also a legal requirement where the processing of personal data is *"likely to result in a high risk to the rights and freedoms of individuals".* If you are unsure whether a DPIA is necessary, you should complete a DPIA screening questionnaire to assess whether the processing you are carrying out is regarded as high risk.

Background

The NHSmail Service a secure email and collaboration service, available for use by local organisations commissioned to deliver publicly funded health and social care in England as approved by the Department of Health and Social Care (DHSC). NHS Digital is the Service Provider for NHSmail Live Service, acting as a Joint Controller with local organisations based in England and Scotland.

NHSmail has been live since 2002 and has over its lifetime changed suppliers and capabilities. It now provides a secure email and collaboration service for all health and care organisations within England and Scotland, that choose to select NHSmail as their secure email platform. NHS Digital is responsible for managing the data processing contract with Accenture (Processor) via a five-year contract (with end date of 31 March 2021). The terms and conditions set out in the contract, which were uplifted in accordance with GDPR in April 2018 (Variation Notice 12), stipulate that data must be processed in accordance with:

• Data Protection Act (1998).

• UK Data Protection Bill (14 Sep 17).

• General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679).

• Data Protection Act (25 May 2018).

Accenture maintain the service via an 'on premise' data centre providing Exchange for email and Skype for business for video consultation. The service plans to move to Exchange online via a cloud-based NHS tenant of Office 365 by October 2020 as a joint venture by NHS Digital, Accenture, and Microsoft. At that point 'Microsoft Teams' will replace 'Skype for business' as the video consultation and online collaboration tool for the NHS.

In March 2020 access to Microsoft Teams was bought forward for NHS organisations to support remote working in response to the 'COVID-19' outbreak, in addition to Microsoft 'OneDrive' and 'Office Online' applications.

This DPIA is published to support local organisations with the completion of their local documentation and guidance for their local GDPR compliance. Information Governance staff, working for local organisations that use NHSmail, can use this DPIA and the wider guidance and policy documents held on the NHSmail Portal support pages to support the completion of local Transparency / Fair Processing Information, guidance and GDPR compliance documentation.

This DPIA covers users in England only in terms of current functionality available and that which is planned in future updates to the service – for detail see **Appendix A.**

In addition to the DPIA a Transparency and fair processing note for NHSmail, as well as roll out information for Office 365 collaboration capabilities, is available from the support pages.

A separate DPIA is available for organisations based in Scotland – who are supported by NHS Scotland Services (NSS).

1. Consultation with Stakeholders

The 2014 supplier and capability change include security and collaboration as the core features and were captured during the procurement phase following widespread consultation:

- Workshops held with Chief Information Officers (CIOs), Royal Colleges and engagement with IT professionals via regional CIO forums.
- End user stakeholder groups.

The NHSmail Live Service contract between NHS Digital (as Joint controller with consumer organisations supporting Health and Social care organisations in England) and Accenture (Processor) sets out the conditions for the service design and the service level agreements (SLAs) that must be met. The contract was finalised following consultation with:

- NHSmail programme leads.
- Accenture programme leads.
- NHS Digital and Accenture legal and commercial teams.
- Department of Health.

Regular user group sessions are held with stakeholder groups to shape and refine the service provision including monthly webinar with Local Administrators, annual all-user survey, and user group workshops.

In March 2020, in response to the Covid emergency Microsoft released Teams for free use. Following discussions between DHSC, NHSX and NHS England, this release was made available through NHSmail.

There is an active user group: -

- The NHSmail Live Service Access Policy sets out the user groups that are served and the Acceptable Use Policy (AUP) provides each individual using the service with details of the terms and conditions by which the service operates.
- For NHSmail policy documentation and guidance visit the NHSmail Portal help pages: https://portal.nhs.net/Help/

In addition to national consultations, local organisations may also hold local consultations with patient groups to explore the use of video and audio conferencing in relation to local information governance policy and procedures in place.

2. Data Flow Diagram

The following diagrams are used to explain data flows.

Figure 1. illustrates data flow and data controller relations

Figure 2. shows boundaries of control

Figure 3. shows boundaries of control in more detail

Figure 4. O365 workload areas with use examples

Figure 5. key data entities with storage setup

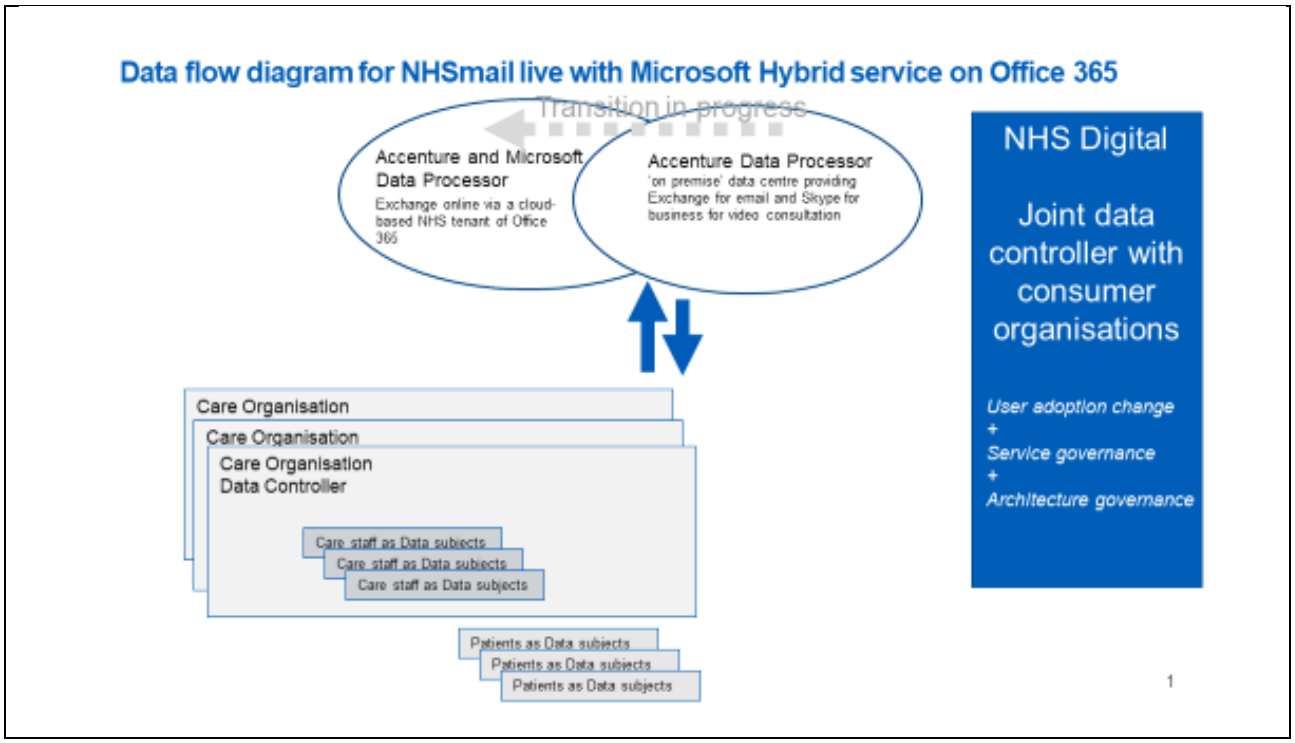

Figure 1. Data flow and data controller relations

There is a complex arrangement for data controller arrangements. The key controllers are the health and care organisations whose staff generate data through use of email and other Office365 tools. NHS Digital is a Joint Data Controller because of its role as the national host organisation for managing commercial relations, funding, technical and service governance and roll out. Accenture is the processor with Microsoft as a sub processor.

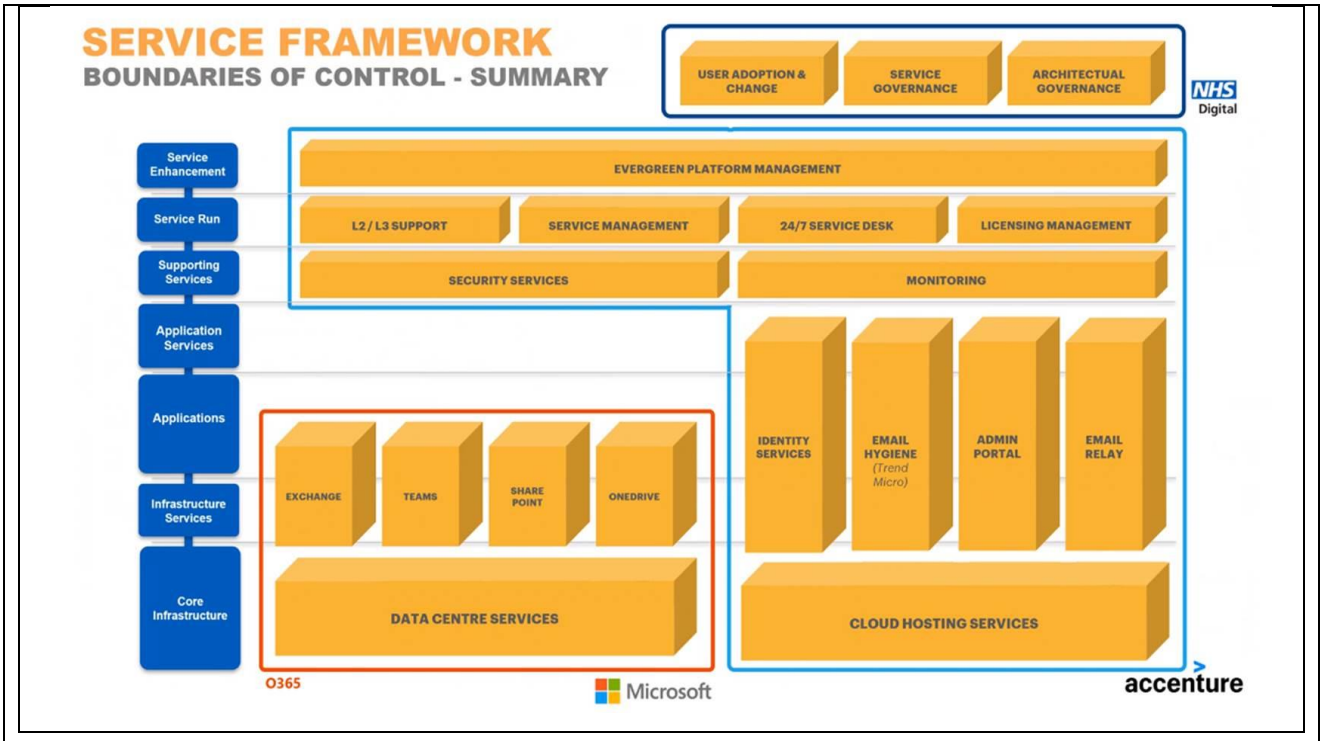

Figure 2. Boundaries of control for care for services provided to health and care organisations by Accenture and NHS Digital

The complexity of data controller relations are managed through services selected by health and care organisations and provided by NHS Digital through Accenture and Microsoft.

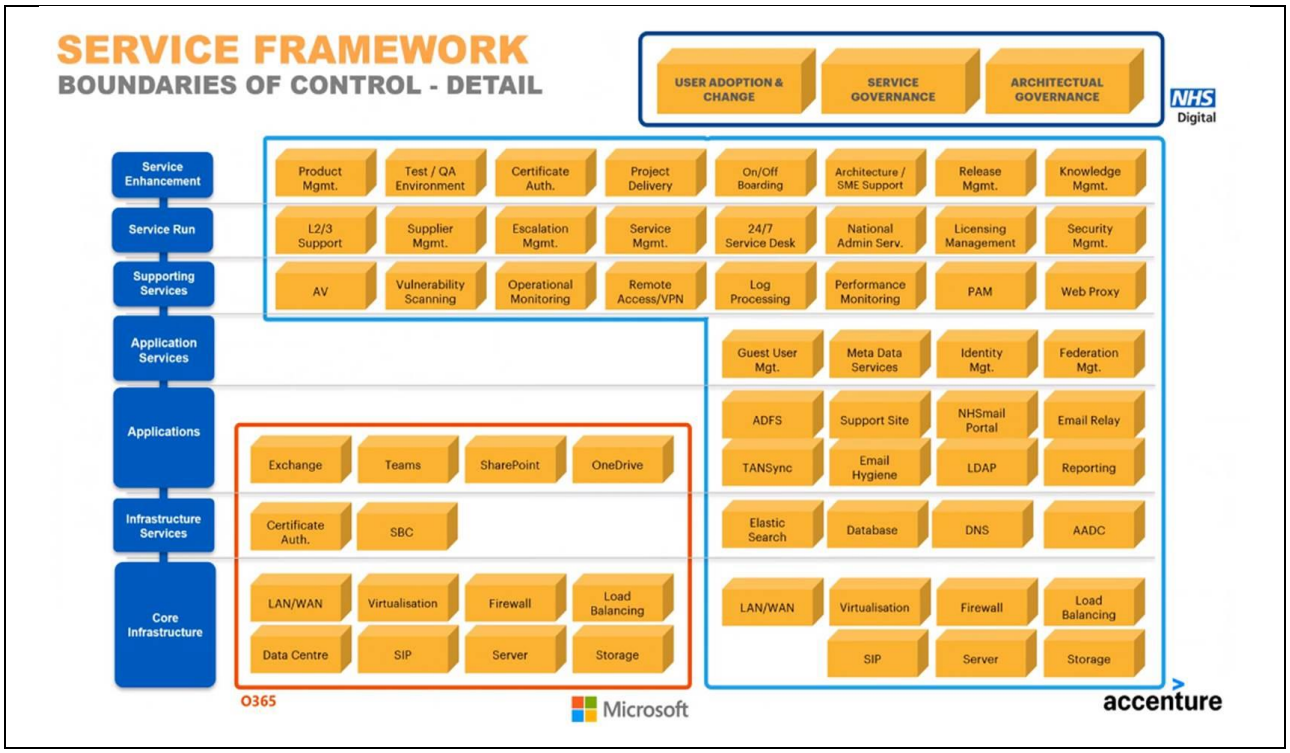

Figure 3. Boundaries of control in more detail

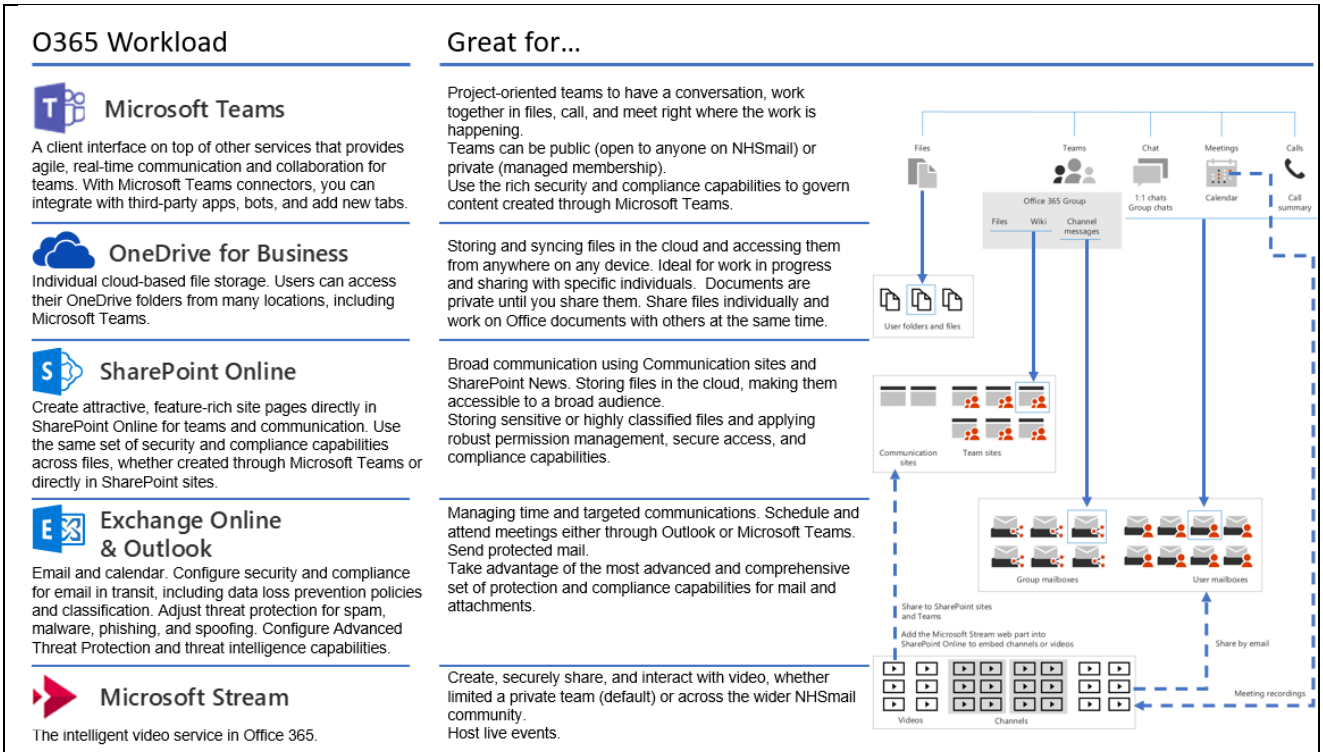

Figure 4. O365 workload areas with use examples for end users

Data Entity Storage

Key data entities and where data is stored at rest

Entity	Storage	Storage
Message	Chat service table storage	Ingested to Exchange to enable compliance
Image	Media service on Azure	Ingested to Exchange to enable compliance
Files	Teams files > SharePoint Chat files > OneDrive for Business	
Voicemail	Individual mailbox in Exchange	
Recording	Media service on Azure	Encoded in Stream
Calendar meeting	Individual mailbox in Exchange	
Contacts	Exchange	
Telemetry	Microsoft Data warehouse (no consumer created content)	

Figure 5. Key data entities with storage setup

3. Purpose of the processing

NHSmail and Office 365 applications provide a range of communication and collaboration capabilities to Health and Care staff. Users and employing organisations are provided with the following benefits:

- Security - NHSmail email sent to secure domains is automatically encrypted and complies with the pan-government secure email standard. NHSmail is accredited to the NHS secure email standard (DCB1596) and is suitable for sharing patient identifiable and sensitive information.

- Collaboration - O365 applications enable secure video conferencing such as MS Teams enabling instant messaging, and file sharing. Increasing productivity, saving time, and allowing staff to work from home and collaborate when required. This allows for the secure transmission of sensitive information related to patient consultations in accordance with guidance set by a local organisations information governance policies and procedures.

- Financial - Because NHSmail and O365 applications are secure they can be used to replace more expensive paper or telephone-based communication processes, saving money that can be better used for patient care.

- Resilient – Service continuity is supported by a range of service level agreements and a dedicated helpdesk 24/7.

- National - Staff can share calendars and folders with any other users on NHSmail, even if they are in different organisations looking up contact details in the NHS Directory of more than one million NHS and business partner staff.

- Safety – Users are protected by sophisticated and up-to-date anti-virus and anti-spam software, which checks every email passing through the NHSmail service.

- Flexibility - NHSmail is a national service, so when organisations merge or re-organise, expensive email migrations are avoided, and users can continue to communicate without disruption.

- Mobility - Access from all common smartphones, tablets, home, and workplace computers, wherever you are in the world. If a mobile device connected to NHSmail is lost or stolen, the information it contains can be remotely erased keeping confidential information safe.

In addition, the service also supports the commitment in the NHS Long term Plan for accelerating digital collaboration within the wider health and social care context.

4. Description of the Processing

Nature and scope of the processing:

There are several types of data:

- NHS Directory and metadata
- Content Stored with NHSmail Services i.e. email, Teams, SharePoint, OneDrive, and Skype message etc.
- Content stored allowing automated updates to NHSmail users (ESR/JML)
- Password synchronisation service allowing organisation local password and NHSmail password to be the same

Detail is provided in **Appendix B.**

The source of this data is those organisations commissioned to support and deliver services across Health & Social care and NHS staff using the service as their primary email product.

In terms of the transition of service provider and model, data is managed by Accenture with Microsoft as a sub-contractor, this will be replaced by use of Exchange online via a cloud-based NHS tenant of Office 365 by October 2020 as a joint venture by NHS Digital, Accenture and Microsoft.

Most personal data is low risk (e.g. name, employer, email address) but there will also be high risk clinical information shared and recorded through email documents and audio and video conferencing. This patient data will include vulnerable groups and, for specialist services, occasionally, reference to criminal offence status.

Data uploaded by users could include any aspect of local NHS business workflows and operations where there is a need to conduct cross working communication and collaboration - this includes the use of patient identifiable data which could be shared with NHS staff.

Users of the service are required to comply with the NHSmail acceptable use policy and governance requirements of the service as well as any existing local information governance policies.

Context of the processing:

NHS Digital is the Service Provider for the NHSmail Live Service, acting as a Joint Controller with local health and care organisations based in England. NHS Digital is responsible for managing the data processing contract with Accenture and Microsoft (Processors)

Microsoft - as a data processor, Microsoft processes user data to provide online services in accordance with instructions from NHS Digital and Accenture. Microsoft also uses personal data to support a limited set of legitimate business operations internally.

Microsoft guidance is available: Data Protection Impact Assessments: Guidance for Data Controllers Using Microsoft Office 365

Local organisations - are responsible for ensuring the data their users store and exchange through the available capabilities are subject to the appropriate internal legal and governance controls. This includes putting a DPIA in place, providing guidance to their users and publishing appropriate privacy information to patients.

Data processing falls into two main categories:

- Data processing by NHS Digital and Accenture to run and maintain the NHSmail Live Service.

- Data processing performed by local organisations using the NHSmail Live Service to share or store data (including patient identifiable data).

Data subjects are local health and care organisations staff and, if the local decision has been made, patients and service users.

A key principle for managing rights of data subjects for NHSmail is the attention and help provided by NHS Digital Live Service and Accenture delivering the service to health and care organisations to ensure transparency to staff and patients is provided and DPIAs are in place. Local transparency, including the data subject rights detailed in Section 13 of this DPIA, what personal data is used/stored and the purposes to which the local organisation shall use their data, is primarily a responsibility of local organisations.

Significant sharing of data is enabled by the O365 tools. This is initiated by the staff employed by local organisations and controlled by the tools (e.g. email and invites for conferencing).

5. Describe the legal basis for the processing (collection, analysis, or disclosure) of personal data?

Health and Social Care Act (2012)

NHS Digital has a legal obligation (a Direction issued by the Secretary of State for Health and Social Care) that requires NHS Digital to establish and operate informatics systems and to exercise systems delivery functions including NHSmail as the national secure email service approved for sharing sensitive information.

Health and Social Care Act (2012) – Section 254, Direction:

> "*Novation of Information and Technology Contracts from DH to NHS Digital: "Electronic Prescription Service, Health and Social Care Network, N3, NHS Choices, NHS e-Referral Service, Secondary Uses Service (SUS), Spine (Named Programmes) Directions 2016*"

NHS Digital (Joint Controller) appointed Accenture as Processor via a commercial contract with an end date of 31 March 2021.)

Microsoft acts as processor due to responsibilities for functionality and licences provided. As specified by the Online Services Terms and Data Protection Addendum, Microsoft, as a data processor, processes Customer Data to provide Customer the Online Services in accordance with Customer's documented instructions

The Azure Active Directory data is processed in UK and USA data centres for resilience and availability as per published - Microsoft guidance on data locations

The service will move to Exchange online via a cloud-based NHS tenant of Office 365 by October 2020 as per a joint venture by NHS Digital, Accenture and Microsoft extending the contract until 31 March 2023.

Additionally, the NHSmail Live Service requires individuals to agree to their personal data being managed by the NHSmail Live Service by accepting the Acceptable Use Policy (AUP) when their account is first initiated. All NHSmail users also have contracts of employment which require maintenance of confidence.

Data Protection Act (2018) and GDPR

NHS Digital and Accenture as supplier of the NHSmail Live Service (as Joint Controller) collects, shares, and processes data within the NHSmail Live Service on the basis of Article 6 (e[1]) and Article 9 (2) (h).

GDPR Article 6: Lawful Processing

Lawful processing by Controller (Article 6 (e);

> (e) Public task - processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

[1] NHS Digital and also applies to health and care organisations

GDPR Article 9: Processing of special categories of personal data

Extract:

Article 9 (2) (h) – processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

Processing:

The NHSmail Live Service establishes email accounts in accordance with the staff details / data provided by local organisations (Joint Controllers), or the individuals themselves, in accordance with Article 9 (2) (h).

The NHSmail Live Service processes patient and confidential information included in secure emails initiated by local organisations (Joint Controllers) for processing by NHS Digital (Processor) and Accenture (Sub Processor) where the data is shared and processed in accordance with Article 9 (2) (h).

Legal basis for – local organisations

Under GDPR legislation local organisations using NHSmail are additionally required to confirm their legal basis for using NHSmail within a locally held Transparency / Fair Processing Information document (also known as Fair Processing Notice) for use by their employees. A local DPIA is also recommended.

The legal basis for local organisations (as the Joint Controller) to share and process data:

1. Lawful processing by Controller (Article 6 (e); *Public task - processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller*

2. Article 9 (2) (h*) – processing is necessary for the purposes of preventive or occupational medicine*, *supplemented by DPA 2018 Schedule 1, Part 2, paragraph 2 - health or social care purposes*

6. Demonstrate the fairness of the processing

Data processing by NHS Digital and Accenture to run and maintain the NHSmail Live Service

A new document has been produced to confirm how the NHSmail Live Service meets the GDPR duty of transparency and is called: NHS Digital (NHSmail Live Service) Transparency / Fair Processing Information.

The NHSmail Live Service has an Acceptable Use Policy (AUP) which staff are required to read and accept before using NHSmail. The AUP sets out the way the service runs, how users are expected to behave, and the data retention periods for data stored about them and the data that they send and receive via the NHSmail service.

Local organisations using NHSmail are required to ensure their staff have read and understood the policy documents and guidance provided by the NHSmail Live Service. The Transparency / Fair Processing Information sets out how the NHSmail Live Service complies with GDPR and should be used by NHSmail users in conjunction with the Transparency / Fair Processing Information provided by their local organisations (as Joint Controllers). There is an active user group in support of local organisations.

Data processing performed by local organisations using the NHSmail Live Service to share or store data (including patient identifiable data)

Local health and care organisations are responsible for briefing data subjects referenced in use of NHSmail and O365 tools.

7. What steps have you taken to ensure individuals are informed about the ways in which their personal data is being used?

Policies, Guidance and AUP

AUP - as stated in Section 7. Policy documentation and guidance is available publicly on the NHSmail Portal help pages setting out how data is collected:

- Data Retention and Information Management Policy
- Access Policy
- Access to Data Policy
- Acceptable Use Policy (AUP)
- NHS Digital (NHSmail Live Service) Transparency / Fair Processing Information
- NHSmail Service: Joint Controller Arrangements

- Welcome Letter: issued when NHSmail account is first setup. Includes links to Portal help pages, training and guidance materials.
- Transparency / Fair Processing Information: advises NHSmail users how their data is captured, used, and stored and supports local organisations with the completion of Transparency / Fair Processing Information notices for their organisation in accordance with their local policies and procedures.
- All user communications: issued at least annually and provide links to Portal help pages.

Local organisations (Joint Controllers) are responsible for ensuring individuals have:

- Accepted and understand the AUP.
- Read and understood the policy documents and guidance published by the NHSmail Live Service on the Portal help pages, including the new Transparency / Fair Processing Information.
- Briefing data subjects referenced in use of NHSmail and O365 tools.

Federation with Partner Organisations

- Federation Partnership Agreements (FPAs) are documents with third party organisations, to agree access and use of the NHSmail Live Service platform specifically for video conferencing and calendar services. Separate agreements are signed with each organisation wishing to federate accepting their responsibilities.

- Data may be provided to other partner organisations governed by the Federation Partnership Agreement.

- Details of organisations that are federated are recorded on the NHSmail Portal help pages.

Local organisations (Joint Controllers) are required to use the Federation Partnership Agreements to inform their local security policies and procedures, which advise their staff which external organisations are suitable for secure collaboration.

8. Is it necessary to collect and process all data items?

For each of the data categories below the justification for collecting, sharing, and processing data falls into two core reasons:

- NHSmail Live Service – account setup. Under joint data controller processing
- NHSmail Live Service – as secure email service (for processing of patient and sensitive data as per Direction from the Department of Health and Social Care and local organisations' selection of NHSmail as their secure email service). This is covered under the jurisdiction of the local organisations IG policy.

The following data categories can be used by NHS Digital (Joint Controllers), local organisations (Joint Controllers) and Accenture (Processor) to setup and manage NHSmail email accounts and collaboration tools provided by the NHSmail Live Service.

Data Categories [*Information relating to the individual*]	**Yes**	**N/A**	**Justifications** *[there must be justification for collecting the data items. Consider which items you could remove, without compromising the needs of the project]*
Personal Data			
Name*	Yes		NHSmail Live Service – account setup
Address	Yes		NHSmail Live Service – account setup - Work address
Postcode	Yes		NHSmail Live Service – account setup - Work address
Date of birth	Yes		NHSmail Live Service – account setup - Data authentication prior to account provision
Professional training / awards	Yes		NHSmail Live Service – account setup - Data authentication prior to account provision
Email address*	Yes		NHSmail Live Service – account setup - Personal email address as data authentication prior to account provision - NHSmail email account stored on NHS Directory
Home phone number	Yes		NHSmail Live Service – account setup - Personal email address as data authentication prior to account provision
Mobile phone / device no*	Yes		NHSmail Live Service – account setup - Personal email address as data authentication prior to account provision - Work contact number stored on NHS Directory
Sensitive Personal Data			
Education / professional training	Yes		NHSmail Live Service – account setup - Personal email address as data authentication prior to account provision - Work role / directorate stored on NHS Directory

*Data elements captured as per the NHSmail account creation and minimum data set

NHSmail Live Service – as secure email and collaboration service

NHSmail Live Service is used by local organisations (Joint Controller) and their users to securely send and receive sensitive or official data (including patient identifiable data).

The following data categories may be included by local organisations (Joint Controllers) within emails or collaboration tools provided by the NHSmail Live Service for processing by Accenture (Processor) to other recipients as directed by the end users and local organisations (Joint Controllers).

NHSmail provides the infrastructure - it is the local organisation IG policy, procedure, and privacy notices for use of data

Data Categories [*Information relating to the individual*]	**Yes**	**N/A**	**Justifications** *[there must be justification for collecting the data items. Consider which items you could remove, without compromising the needs of the project]*
Personal Data			
Name	Yes		NHSmail Live Service – presence of this and other items are a decision of each NHSmail service user within the constraints of their employing organisation
Address	Yes		NHSmail Live Service – as above
Postcode	Yes		NHSmail Live Service – as above
Date of birth	Yes		NHSmail Live Service – as above
Age	Yes		NHSmail Live Service – as above
Sex	Yes		NHSmail Live Service – as above
Marital status	Yes		NHSmail Live Service – as above
Gender	Yes		NHSmail Live Service – as above
Living habits	Yes		NHSmail Live Service – as above
Professional training / awards	Yes		NHSmail Live Service – as above
Income / financial / tax situation	Yes		NHSmail Live Service – as above
Email address	Yes		NHSmail Live Service – as above
Physical description	Yes		NHSmail Live Service – as above
General identifier e.g. NHS no.	Yes		NHSmail Live Service – as above
Home phone number	Yes		NHSmail Live Service – as above
Online identifier e.g. IP address / event logs	Yes		NHSmail Live Service – as above
Mobile phone / device no.	Yes		NHSmail Live Service – as above
Device mobile phone / device IMEI no.	Yes		NHSmail Live Service – as above
Sensitive Personal Data			
Physical / mental health or condition	Yes		NHSmail Live Service – as above
Sexual life / orientation	Yes		NHSmail Live Service – as above

Data Categories [*Information relating to the individual*]	**Yes**	**N/A**	**Justifications** *[there must be justification for collecting the data items. Consider which items you could remove, without compromising the needs of the project]*
Family / lifestyle / social circumstance	Yes		NHSmail Live Service – as above
Offences committed / alleged to have committed	Yes		NHSmail Live Service – as above
Criminal proceedings / outcomes / sentence	Yes		NHSmail Live Service – as above
Education / professional training	Yes		NHSmail Live Service – as above
Employment / career history	Yes		NHSmail Live Service – as above
Financial affairs	Yes		NHSmail Live Service – as above
Religion or other beliefs	Yes		NHSmail Live Service – as above
Trade Union membership	Yes		NHSmail Live Service – as above
Racial / ethnic origin	Yes		NHSmail Live Service – as above
Genetic data	Yes		NHSmail Live Service – as above

9. Describe if personal datasets are to be matched, combined, or linked with other datasets? (internally or for external customers)

Personal Staff Data

Data about staff is stored against their NHSmail account including information such as name, telephone number, job role. This data is visible to the NHSmail user via the NHSmail Portal in the NHS Directory and can be updated and changed by the user as required via a request to an employing local organisations IT department.

Each of these individual entries are available in a single Directory (NHS Directory) to all NHSmail users and not publicly available. It is the responsibility of the employing organisation to ensure data uploaded to the NHS Directory remains up to date and accurate.

Link to Electronic Staff Record (ESR)

Local organisations may use the connector service (TANsync) to maintain staff details which will match / combine data supplied by the local organisation or ESR.

In relation to ESR, NHS Digital have an agreed Data sharing agreement with NHS Business Services Authority (NHSBSA)(the ESR controlling organisation) for the processing of the ESR extract. The request for the extract file that NHSmail processes is made through ESR by the requesting NHS organisation. Part of this process informs the NHS organisation of their responsibilities and obligation under GDPR (noted here for completeness). This service is a requested opt in service on NHSmail.

Official Data

NHSmail is used by local organisations to send / receive data including patient / service user / client identifiable data and related health and social care data. Includes sensitive data.

Organisations use the NHSmail Live Service in line with their local policies and procedures which could involve this class of data. For example, sending patients appointment reminders, archiving emails according to local data storage procedures.

NHSmail supports open APIs, allowing organisations to programmatically send / receive secure data to / from other systems (such as e-referral systems).

Local organisations using APIs to extract personal data or official data from the NHSmail Live Service are required to protect and secure this data via their local processing standards and policies. Once data is extracted, the local organisation becomes the Controller for this data.

Recorded content

Should local care organisations select to use MS Teams for audio and video conferencing patient information may be recorded by the Teams application. Further information around Teams use has been provided via the NHSmail support site.

These can be associated with the relevant patient record held within the local care organisation and is the responsibility of the local care organisation to manage and use in relation to local information governance policy and procedures.

10. Describe if the personal data is to be shared with other organisations and the arrangements you have in place

See section 9 – NHS Directory, local choice of use of ESR to support maintenance of user base with staff changes.

11. How long will the personal data be retained?

Patient Data

Should local care organisations select to use MS Teams for audio and video conferencing patient information may be recorded. Recorded data can be associated with the relevant patient record held within the local care organisation and manged as per local information governance policies and procedures.

User data will remain until deleted. For example, a Multi-Disciplinary Team (MDT), hosted in MS Teams could contain patient data during the meeting, which should then be transferred to the patient record.

Any data that resides in O365, including patient data, is the responsibility of local organisations and is subject to local information governance and clinical safety practices. Local organisations must update transparency information to record how this data is captured and stored.

Personal Staff Data

Data about staff is stored for as long as the account is active. For account status definition and lifecycle please see the below Data Retention and Information Management Policy.

An account will remain active if it has been logged into, had a password change, or sent an email within the last 365 days.

As part of an official investigation, data within the retention period of 180 days (since last edited) can be accessed for the following Office 365 applications (when enabled):

- OneDrive for Business accounts
- SharePoint site collections
- Office 365 groups (including emails to groups, conversation and files transferred in Teams channels conversation and file transfer)
- Teams private (one-to-one) conversation (IM only)
- Recorded Teams conversations available via the application Stream

NHSmail Email Data

The NHSmail Data Retention and Information Management Policy sets out data storage periods for the service.

Centrally, copies of email sent / received are retained for 180 days for forensic audit purposes and message summaries for two years. Organisations use the NHSmail Live Service in line with their local policies and procedures which could involve storage of data locally for more than two years.

Leaver Policy

NHSmail accounts transfer between organisations using the Leavers, Joiners and transfer Management Policy, allowing individuals to keep the same email account throughout their career.

Local organisations (Joint Controller) are required to set guidance for staff that leave their organisation to retrieve any relevant data that is held within the NHSmail user account prior to their departure. This data will also be stored centrally, as described above, in accordance with the Data Retention and Information Management Policy.

Forensic requests for staff that have left can still be submitted by local organisations (Joint Controllers) for the periods of employment that apply.

NHS Directory

The NHS Directory information is retained for as long as the account is active. Local organisations (Joint Controller) responsible for maintaining / deleting contact details held on the NHSmail Directory – known as NHS Directory.

Other

The service retains audit logs about individual users and their access to the service. These are described in the Data Retention and Information Management Policy.

Users calling the NHSmail helpdesk should note that all calls are recorded and stored for two months for quality purposes

12. Where you are collecting personal data from the individual, describe how you will ensure it is accurate and if necessary, kept up to date

Personal Data

Personal data can be edited by the local organisations (Joint Controller) to ensure records are kept current.

NHS Directory and NHSmail Portal

This is maintained by the administrators in the local organisation employing the member of staff, it may be maintained either through the NHSmail Portal or through an automated synchronisation from a local directory (i.e. with TANSync). For certain fields (i.e. telephone number) the user can update these themselves through self-service.

Email, Video conferencing and other collaboration data

Data quality for content sent over email or Video conferencing capabilities or stored within other collaboration tools is the responsibility of the user sending / uploading the information. In the event it is incorrect the user should update and re-send / upload the corrected information.

13. How are individuals made aware of their rights and what processes do you have in place to manage such requests?

Local user organisations (Joint Controllers) are responsible for providing Transparency / Fair Processing Information to those affected by the processing and having procedures in place to ensure the rights provided by the appropriate legal basis can be exercised.

The NHSmail Live Service, on the legal basis of “legal obligation”, upholds the following rights:

- Right to be informed
- Right of access
- Right to rectification
- Right to restrict processing – where an individual has objected to the processing and you are considering whether your organisations legitimate grounds override those of the individual.
- Right to object (based on grounds relating to his or her particular situation) – unless you can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or the processing is for the establishment, exercise or defense of legal claims
- Right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her (unless processing is necessary for reasons of substantial public interest)

In addition, individuals who are not satisfied with the response from the NHSmail Live Service or believe their data is not being processed in accordance with the law, can complain to the Information Commissioner’s Office (ICO) which is the regulator for Data Protection and upholds information rights. More information is available on the ICO website https://ico.org.uk/

How individuals can exercise these rights is described in the Transparency / Fair Processing Information provided to all users.

Process Summary

Rights	How upheld by NHSmail Live Service	Local organisation responsibilities
Right to be informed	NHS Digital: NHSmail Live Service Transparency / Fair Processing Information advises NHSmail users how their data is captured, used and stored and supports local organisations with the completion of Transparency / Fair Processing Information notices for their organisation in accordance with their local policies and procedures	Transparency / Fair Processing Information must be provided to NHSmail users setting out how local policies and procedures apply to the capture, use and storage of their data.
Right of access	NHSmail Live Service manage high volumes of data across the service. Local organisations must have their own policies and procedures in place that align to agreed national processes across NHSD and Accenture.	Requests should be made to the NHSmail Local Administrator within the health and care organisation that owns your NHSmail account following agreed local and national processes.
Right to rectification	If the NHSmail Live Service has recorded your personal details within the service, including the NHS Directory, incorrectly or it is incomplete, you can make a request to your NHSmail Local Administrator	Local Administrators are responsible for supporting NHSmail users to make the necessary amendments. Guidance on finding your Local Administrator is available.

	or the NHSmail helpdesk who can make the necessary amendments. Guidance on finding your Local Administrator is available.	
Right to restrict processing – where an individual contests the accuracy of the personal data, processing should be restricted until accuracy has been verified	NHSmail Live Service manage high volumes of data across the service. Local organisations must have their own policies and procedures in place that align to agreed national processes across NHSD and Accenture. A condition of using NHSmail is that the NHS Directory is populated with user information as it is not possible to operate the service without it.	Requests should be made to the NHSmail Local Administrator within the health and care organisation that owns your NHSmail account following agreed local and national processes
Right to object (based on grounds relating to his or her particular situation) – unless you can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or the processing is for the establishment, exercise or defence of legal claims	NHSmail Live Service manage high volumes of data across the service. Local organisations will have their own policies and procedures in place that will align to agreed national processes across NHSD and Accenture. A condition of using NHSmail is that the NHS Directory is populated with user information as it is not possible to operate the service without it.	Requests should be made to the NHSmail Local Administrator within the health and care organisation that owns your NHSmail account following agreed local and national processes
Right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her (unless processing is necessary for reasons of substantial public interest)	NHSmail Live Service manage high volumes of data across the service. Local organisations will have their own policies and procedures in place that will align to agreed national processes across NHSD and Accenture. A condition of using NHSmail is that the NHS Directory is populated with user information as it is not possible to operate the service without it. Data is held confidentiality and securely.	Requests should be made to the NHSmail Local Administrator within the health and care organisation that owns your NHSmail account following agreed local and national processes Each employing organisation will have local policies and policy that should be read and understood.

Requests for an NHSmail account to be removed are processed by the Local Administrators, National Administration Service (Accenture) or the National helpdesk (Accenture), using the standard leavers' process. Requests from individuals to be immediately deleted (forgotten) will be considered in accordance with Article 17 GDPR subject to authorisation from the local organisation (Joint Controller) where the individual was employed.

Requests for hiding an individual from the NHS Directory require permissions from the owner or HR director to be forwarded to the NHSmail Live Service Operations Team (NHS Digital) via feedback@nhs.net before the NHSmail helpdesk (Accenture) can action. Urgent requests can be processed by logging the information with the NHSmail Operations Team while raising a service request in parallel.

14. What technical and organisational controls for "information security" have been put in place?

The NHSmail Live Service is accredited to the NHS secure email standard and is compliant with ISO27001 and a number of security standards.

Accreditation	Certificate Number
ISO 9001:2015	FS 571552
ISO/IEC 20000-1:2011	ITMS 535634
ISO/IEC 20000-1:2011	ITMS 571355
ISO 22301:2012	BCMS 523309
ISO 22301:2012	BCMS 556058
ISO/IEC 27001:2013	IS 589293

These certificates can be viewed via the BSI validation tool.

The NHSmail Live Service is audited on an annual basis (IT Health Check or Pen Test) by an independent organisation to ensure security standards and service levels are maintained at the highest possible levels.

A System Level Security Policy (SLSP) is in place between NHS Digital (Joint Controller) and Accenture (Processor) which captures the system infrastructure and security protocols in place for the NHSmail Live Service. This is a commercially sensitive document which cannot be shared. NHS Digital, as Joint Controllers, manage the SLSP on behalf of local organisations (Joint Controllers).

The NHSmail helpdesk and service management for the NHSmail Live Service operate in accordance with the ITIL service management framework. Accenture are fully compliant with the ISO20000-1:2011 Service Management System (SMS) standard and are annually re-accredited to confirm continued compliance by an independent business standards organisation (BSI).

The NHSmail Live Service Technical Design Authority (TDA) has responsibility for overseeing design changes and proposed developments to the service. The TDA ensures all changes are:

- Secure by design and maintain accreditation to the secure email standard.
- Maintain the integrity of the Core Service design as contracted.
- Align to Information Governance Standards.
- Align to accreditation certificates (as listed above).

TDA recommended changes are approved by the NHSmail Board (chaired by NHSmail Product Owner) and are implemented by Request for Change (RFC) notices.

Contractual

A GDPR Compliant Contract is in place between NHS Digital (Joint Controller) and Accenture (Processor). The NHSmail Live Service contract includes Service Level Agreements (SLAs) which Accenture (Processor) are required to uphold. The NHSmail Live Service contract, and these SLAs, are managed by NHS Digital (Joint Controller) on behalf of all Controllers. The SLA status is published on the NHSmail Portal help pages.

Information Governance (IG)

Local organisations (Joint Controllers) are required to complete an annual toolkit return to ensure that NHSmail users have completed IG training. To access NHSmail, health and care organisations must meet **or exceed** one of the following:

- A Data Security and Protection Toolkit rating of 'Entry Level'. Please note a rating of 'Entry Level' is a minimum and will not be sufficient to meet wider contractual and regulatory requirements or the requirements to connect to other NHS Digital services.

New organisations joining NHSmail are required to self-declare IG compliance before NHSmail accounts are authorised.

Local organisations (Joint Controllers) appoint Local Administrators (LAs) to manage and maintain the NHSmail service for their organisation including the adding, removal and suspension of NHSmail accounts. Local Administrator guidance is provided via the NHSmail Portal help pages, monthly webinars and bulletins.

OR

Local organisations (Joint Controllers) are required to appoint shared mailbox owners (privacy officers) to oversee the IG and data management for their site. These arrangements are typically for smaller organisations that:

- Utilise the National Administration Service (NAS) provided by Accenture (through contract with NHS Digital as Joint Controller) or
- Appoint a Local Sponsoring Organisation (e.g. clinical commissioning group) to provide the administration and maintenance of the email accounts and collaboration tools.

Shared mailbox guidance is provided via the NHSmail Portal help pages and user group specific bulletins.

System Security

The NHSmail service includes a number of security features intended to prevent the transmission and storage of SPAM or malware through the platform. It also includes various security monitoring technologies to detect attacks or abuse of the system.

15. In which country/territory will personal data be stored or processed?

See Appendix C

16. Does the National Data Opt Out apply to the processing?

The NHS Opt-out does not apply to the three types of data:

- Data processing by NHS Digital and Accenture to run and maintain the NHSmail Live Service.
- Data processing performed by local organisations using the NHSmail Live Service to share or store data (including patient identifiable data).
- Clinical data created in O365 should be moved to the clinical record and any national data opt out considerations should be addressed in the clinical record repository

17. Identify and assess risks

Consider the potential impact of your processing and the potential harm or damage that it might cause to individuals whether physical, emotional, moral, material or non-material e.g. inability to exercise rights; discrimination; loss of confidentiality; re-identification of pseudonymised data, etc.

You can also use this section to detail any risks you have in complying with data protection law and any resulting corporate risks e.g. impact of regulatory action; reputational damage; loss of public trust, etc.

Describe source of the risk and nature of potential impact on individuals	**Likelihood of harm** (Remote; reasonable possibility or more likely than not)	**Severity of impact** (Minimal impact; some impact; or serious harm	**Overall risk rating** (Low; medium; or high)
Impact to individual from delay in processing data for a subject access request.	Remote	Some impact	Low
High severity service incidents either locally e.g. network issue or nationally e.g. server outage could impact the ability to process subject access requests by the NHSmail supplier	Remote	Some impact	Low

Local NHS organisations not having their own local IG policy/procedure in place to support the processing of requests or to meet transparency obligations under GDPR.	Remote	Some impact	Low
When an employee, employed by Organisation ”A”, moves to Organisation “B”, the employee is permitted, due to their email account contents not being purged, to take with them the personal data for which Organisation “A” remains the “Controller”.	Remote	Some impact	Low

17.1. Measures to mitigate (treat) risks

Against each risk you have identified, record the options/controls you have put in place to mitigate the risk and what impact this has had on the risk. Make an assessment as to the residual risk.

Also indicate who has approved the measure and confirm that responsibility and timescales for completion have been integrated back into the project plan.

Risk	**Options to mitigate (treat) the risk**	**Effect on risk** (Tolerate / Terminate / Treat Transfer)	**Residual risk** (Low / Medium / High)	**Measure approved** (Name and Date)	**Actions integrated back into project plan** (Date and responsibility for completion)
Impact to individual from delay in processing data for a subject access request.	Local Administrator responsibilities are reiterated through bulletins, webinars, and guidance available on the NHSmail support pages. The services ‘Access to data policy’ is	Tolerate	Low	Chris Parsons May 2020	Ongoing BAU

	available from the NHSmail support pages. Urgent requests received for statutory deadlines are prioritised.				
High severity service incidents either locally e.g. network issue or nationally e.g. server outage could impact the ability to process subject access requests by the NHSmail supplier	Organisations must ensure they have local policies in place to mitigate any high severity service incidents affecting their ability to process requests. The NHSmail service has a high level of contractual service level agreements in place to ensure continuity of the NHSmail service. High severity incidents are rare and to date have had no impact on the services ability to process subject access requests made by local organisations.	Tolerate	Low	Chris Parsons May 2020	Ongoing BAU
Local NHS organisation not having their own local IG policy/procedure in place to support the processing of requests.	Refer local NHS organisations and local administrators to NHSmail information management policies https://support.nhs.net/article-categories/information-management-policies/ Reiterate local NHS organisation responsibly to ensure local IG policy and procedure in place to support requests.	Tolerate	Low	Chris Parsons May 2020	Ongoing BAU
Impact to individual data from user belonging to a new organisation and having access to email account where previous organisation remained the data controller.	• NHSmail publishes policy and guidance for how local NHS organisations can support via the joiners and leavers guide (https://support.nhs.net/knowledge-base/leavers-and-	Tolerate	Low	Chris Parsons May 2020	Ongoing BAU

	joiners-guide/) which sets out specific tasks that LAs must do in the event someone leaves their organisation • The NHSmail Acceptable Use Policy must be accepted by a user prior to a user sending any email. The policy states to follow IG policies of the local organisation and ensure personal email is clearly identified • Information requests require authorisation from a requesting CEO/HR Director as approvers to ensure disclosure is deemed valid and appropriate • Requests will only be accepted from the current owning organisation where the account resides • Future NHSmail capability will allow user account data to be purged by a local administrator as part of a local leaver process				

18. Further Actions

- The IAO should keep the DPIA under review and ensure that it is updated if there are any changes (to the nature of the processing and/or system changes)

19. Signatories

The DPIA accurately reflects the processing and the residual risks have been approved by the Information Asset Owner:

Information Asset Owner (IAO) Signature and Date

Chris Parsons
Associate Director Solutions Assurance (ai)
Programme Head/Product Owner
Digital Collaboration/NHSmail

02 June 2020

FOR OFFICE OF THE SIRO AND OFFICE OF THE DPO USE ONLY

20. Summary of high residual risks

Risk no.	High residual risk summary

Summary of DPO advice:

Data Protection Officer (DPO) **Signature and Date**

Kevin Willis Data Protection Officer NHS Digital	29.05.2020

ICO consultation outcome:

Office of DPO **Signature and Date**

Judged as not required.

Next Steps:

- **Continue to review DPIA in relation to NHSmail with O365 capability releases**

Appendix A

NHSmail current functionality available and planned for future updates

NHSMAIL REFRESH
CAPABILITY RELEASE PLAN

Product	Capability	National Release Status
Office 365	Microsoft Teams – Conferencing, meetings, IM/presence, chat, collab.	AVAILABLE
	Teams Live Events	AVAILABLE
	OneDrive for Business – personal online document storage	AVAILABLE
	SharePoint - Team collaboration & internal portals	AVAILABLE
	Office Online – Create/edit rights for online versions of core Office apps	AVAILABLE
	Office Mobile Apps – Create/edit rights for commercial use	AVAILABLE
	Dial In Audio Conferencing	AVAILABLE
	B2B Collaboration	AVAILABLE
	Microsoft Stream	AVAILABLE
	Microsoft Bookings	NHSmail Refresh
	Microsoft Planner	NHSmail Refresh
	To-Do – Personal task management app	NHSmail Refresh
	Shift scheduling, content sharing, and workgroup messaging	NHSmail Refresh
	PowerApps and Flow	NHSmail Refresh
	Sway for Office 365	NHSmail Refresh
	Microsoft Forms	NHSmail Refresh
	Yammer	NHSmail Refresh
	Install Office on up to 5 PCs/Macs + 5 tablets + 5 smartphones per user	Local License top-up

Appendix B

Data processing table

Category	**Who's information**	**System**	**Where is it going**	**Nature and Purpose of the Processing**	**Frequency** e.g. daily, weekly, monthly, real time	**Method of transport** Electronic system transfer, Fax, Secure Email, Paper or shared drive, Post	**PID/ No PID**	**Type of information** e.g. letter, report, referral, or patient history
NHS Directory and metadata	Controller staff, Controller Service Recipient	NHSmail and Office 365	Stored within NHSmail in the UK and USA. May be viewed outside of the EU.	Administration of services provided by NHSmail	Real-time	Electronic system transfer - EST	PID	Business identifiers - email address, - telephone number - organisation First Name Last Name
Content Stored with NHSmail Services i.e. email, Teams messages etc.	Controller staff, Controller Service Recipient staff, NHS patients, member of the public	NHSmail and Office 365	Stored within NHSmail in the UK. May be viewed or transmitted outside of the EU.	Processing and storage of email and data being shared across all O365 products (See annex C) .	Real-time	Electronic system transfer - EST	PID	Patient identifiable data which may include reports, medical images, passport detail copies, financial data, other personal identifiers.
Content stored allowing automated update of NHSmail users (ESR/JML).	Controller staff, Controller Service Recipient	NHSmail	Stored within NHSmail in the UK. May be viewed outside of the EU.	Processing of Electronic Staff Record for the automated update of NHSmail accounts and local directory services e.g. Active Directory	Daily	Electronic system transfer - EST	No PID	Business identifiers - email address, - telephone number - organisation First Name Last Name
Password synchronisation service allowing organisation local password and NHSmail password to be the same	Controller staff, Controller Service Recipient	NHSmail and local directory service	NHSmail password stored within NHSmail in the UK. Synchronised with the local directory password within the UK.	Facilitating the ability to synchronise passwords between NHSmail and local directory services	Real-time	Secure electronic transfer - EST	No PID	Password

Appendix C

NHSmail Office 365 applications data by location

Data is stored / processed by Microsoft by application, in the following locations:

Exchange Online	United Kingdom
OneDrive for Business	United Kingdom
SharePoint Online	United Kingdom
Skype for Business	United Kingdom
Azure Active Directory*	United Kingdom, United States
Microsoft Teams	United Kingdom
Office Online	United Kingdom
Office Mobile	United Kingdom
EOP	United Kingdom
MyAnalytics	United Kingdom
Planner	European Union
OneNote Services	United Kingdom
Stream	United Kingdom
Yammer	European Union
Sway	United States
Whiteboard	European Union
Forms	European Union

- Applications above where data does not reside in the United Kingdom will be disabled by default by NHS Digital. If required, an organisation will need to enable these on a per user basis aligned to local legal/information governance advice, ensuring it has met the requirements in the GDPR and the Data Protection Act and locally agreed policies and procedures
- United Kingdom refers to data which is stored in either Durham, London, or Cardiff.

* The Azure Active Directory data is processed in UK and USA data centres for resilience and availability as per published - Microsoft guidance on data locations