Joint Controller Arrangement Table

Roles and responsibilities in relation to the NHSmail O365 shared tenant live service

Published July 2021

Version 1.0

Contents

1. Introduction

This Joint Controller Arrangement Table (**Table**) sets out the roles and responsibilities under Article 26 of the UK General Data Protection Regulation ("**UK GDPR**") of the following parties:

- NHS Digital (known in statute as the Health and Social Care Information Centre); and
- The health and social care organisations consuming and operating NHSmail at a local level ("**Local Organisations**"),

in relation to the processing of personal data through the delivery, maintenance and operation of the secure email and collaboration live service known as the NHSmail O365 shared tenant, hereafter referred to as 'NHSmail'

In setting out these roles and responsibilities, it is important to note that NHSmail is primarily designed to operate as a communication tool to support the secure exchange of information between health and care professionals. It is not designed to act as a document management system and should not be relied upon as such, as there are limits to the storage capabilities of NHSmail due to the high volumes of data generated through the service. NHS Digital provides additional support to Local Organisations to enable them to fulfil their responsibilities at a local level, through the development, testing and assurance of new functionality and publication of central guidance and policy, such as the NHSmail Clinical Safety Case and the NHSmail Data Protection Impact Assessment which can be used in the production of local guidance and documentation as necessary.

Given that one of the primary functions of NHSmail is to support health and care staff, a large proportion of the personal data collected through this service will relate to the personal data of patients (including health data) and staff. As a result, Local Organisations should be acutely aware of their legal and service responsibilities as to the collection, use, storage and suitable management of personal data.

The commercial agreement for NHSmail originated as a contract for the provision of a managed email system between the Department of Health and Social Care ("**DHSC**") acting as a controller, and the main supplier, Accenture, acting as a processor.

In response to the novation of information and technology contracts from DHSC 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 ("**the 2016 Directions**"), the contract and public legal function associated with NHSmail was novated from DHSC over to NHS Digital (now acting as controller) to continue the contract with Accenture (who continue to act as processor). As a result, DHSC retained no residual responsibility or involvement since the novation was executed.

2. The UK GDPR

The purpose of this Table is to set out the Joint Controller Arrangement between the bodies listed above in relation to the NHSmail service in order to clarify roles and responsibilities for the purposes of Article 26 of the UK GDPR.

Article 26 of the UK GDPR governs the relationship between Joint Controllers. Article 26(1) of the UK GDPR provides that "*where two or more controllers jointly determine the purposes and means of processing, they shall be Joint Controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by domestic law. The arrangement may designate a contact point for data subjects.*"

Under Article 26(2) of the UK GDPR, "*the arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the Joint Controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject*".

2.1 Transparent manner

The Table below can be referred to in relevant Data Protection Impact Assessments ("**DPIAs**"). It will also act as a stand-alone document which can be issued to anyone who requests it. It transparently sets out each party's respective obligations and responsibilities as Joint Controllers for the NHSmail service.

2.2 Respective Responsibilities for Compliance in particular with regard to exercise of data subject right and duties to provide information in Articles 13 and 14

The Table below sets out each Controller's responsibilities for:

- compliance with the obligations under UK GDPR which apply to controllers;
- compliance with Article 13 and Article 14 of the UK GDPR; and
- compliance with the exercise of data subject's rights.

This Table constitutes the arrangement referred to in Article 26.

2.3 The arrangement may designate a contact point for data subjects

NHS Digital is designated as the contact point, for data subjects in the Table below and in the NHSmail Transparency Notice, in relation to its role as the National Host Organisation (see definition below) of the NHSmail service. NHS Digital's Data Protection Officer is also named in the NHSmail Transparency Notice as a contact point.

The Local Organisation consuming, and therefore becoming a local provider of, the NHSmail service is also designated as the contact point, for data subjects in relation to its management of the service at a local level and should be the primary point of contact for a service user under that Local Organisation's use of the service. This is because Local Organisations are responsible for the management of individual accounts under that local use of NHSmail. Further to this, Local Organisations are responsible for setting out the personal data categories it decides to process under its local use of the service. As a result, each Local Organisation is primarily accountable for the data processing it undertakes in its use of the service and hence should be the primary contact point for users under that local use of NHSmail. The NHSmail support site provides guidance for local administrators - Administrator Guide – NHSmail Support.

The above information should be set out in each individual Local Organisation's Transparency Notice. The Local Organisation's Data Protection Officer should also be named in each individual Local Organisation's Transparency Notice as a contact point.

2.4 The arrangement will reflect the respective roles and relationships of the Joint Controller vis-à-vis the data subjects

The Table and the two Transparency Notices referred to above reflect these roles. NHS Digital is identified as the Controller who processes the personal data as the national provider of the NHSmail service, including capturing, using, storing data and providing the infrastructure to support local organisations with their use of NHSmail ("**National Host Organisation**"). In relation to this processing, NHS Digital is the contact point for data subjects to exercise their rights under the NHSmail Transparency Notice.

The Local Organisation is identified as the Controller who processes through capturing, using and storing data through providing the NHSmail service a local level ("**Local Service Provider**"). Local Organisations use the infrastructure provided by NHS Digital to provide their own local NHSmail service to the organisation they are responsible for. Local Organisations have the discretion to use parts of the service (instances set out in the Table below) in a manner most suitable to them, as long as these are aligned to sit within the national framework that has been provided and are documented in local IG policies, procedures and privacy notices. As a result, Local Organisations will be the primary contact point for service users in relation to the local application of the service.

2.5 The essence of the arrangement shall be made available to the data subject

The essence of this arrangement is described in the Transparency Notices referred to above. The NHSmail Transparency Notice (in relation to NHS Digital's role as the National Host Organisation) is publicly available on the NHSmail support site.

The Local Organisation Transparency Notice can be provided to data subjects on request to the Local Organisation.

Data subject rights in relation to NHSmail apply to service user and patient data subject rights as well as NHSmail users. However, it should be noted that this is a communication tool, not a medical record. Any amendments by a data subject to their patient medical record should be done through the appropriate system. The reference to data subject rights set out in the Table below are purely in relation to data contained in the NHSmail system.

3. Key to roles and responsibilities

To assist, where a party:

- has compliance responsibilities this has been identified with a ✓
- does not have compliance responsibilities, this has been identified with a ✗

UK GDPR Requirement	NHS Digital (acting as National Host Organisation)	Local Organisations (acting as Local Service Provider)
The Controllers	The Health and Care Information Centre, known as NHS Digital 7 & 8 Wellington Place Leeds West Yorkshire LS1 4AP ICO Registration No: Z8959110 https://ico.org.uk/ESDWebPages/Entry/Z8959110 NHS Digital has a legal obligation 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 under the 2016 Directions, as directed by the Secretary of State of Health and Social Care under s.254 of the Health and Social Care Act 2014. Due to the 2016 Directions, NHS Digital acts as National Host Organisation of NHSmail. It also acts as a Joint Controller of NHSmail with Local Organisations, who consume this service. In order to implement NHSmail, NHS Digital has in place a commercial contract with Accenture, who it instructs as a Processor, to assist with the delivery of NHSmail. This contract currently has an end date of 21 March 2023.	Local Organisation - e.g. NHS trust, health board, NHS England local area team, Commissioning Support Unit, Clinical Commissioning Group (and GP practices in its designated local area), other eligible non-departmental public bodies (such as NHS Blood & Transplant, NHS BSA, NHS Counter Fraud Authority etc.), GP locums, pharmacy, dentistry and social care managed by the National Administration Service (NAS). NHS Digital is also an organisation that consumes the NHSmail service and so it does act as a Local Organisation in respect of its local use. In respect of this separate role to acting as the National Host Organisation, it carries the same responsibilities to that of a Local Organisation. The Local Organisation is also a Joint Controller by virtue of consuming the NHSmail service maintained and implemented at a local level relevant for the use of that Local Organisation. The scope of organisations able to consume NHSmail are broad in size and purpose and as a result, Local Organisations should develop local policies and procedures that set out how they should capture, use, store and, where applicable, share data in their use of the service. Local Organisations are expected to work within the agreed national processes where they exist (e.g. giving data subjects a right of access / document retention). However, due to the variation amongst Local Organisations, NHSmail cannot operate a ‘one size fits all’ approach and Local Organisations do have discretion as to how they operate the service at a local level, for example what data categories it chooses to process as part of the email system and collaboration tools it operates at a local level. As the primary customers of NHSmail, the legal power for NHS trusts to use this service and act as Joint Controllers comes from Schedule 4 of the Health and Social Care Act 2006. Paragraph 14(1) of this Schedule provides that “an NHS trust may do anything which appears to it to be necessary or expedient for the purposes of or in connection with its function”. With regard to the joint exercise of functions, Paragraph 18 of the same Schedule provides that “an NHS trust may enter into arrangements for the carrying out, on such terms as the NHS trust considers appropriate, of any of its

				functions jointly with any Special Health Authority, Local Health Board or other NHS trust, or any other body or individual". With regard to the remainder of Local Organisations utilising the NHSmail service, as they are public bodies they will each have a legal power allowing them to act in a way which is necessary or expedient to their function. It is for these organisations to set out their legal basis for processing in their Transparency / Fair Processing information. Further to the above, it is the responsibility of Local Organisations to ensure that the individual users comply with the service terms relating to responsible use of NHSmail as set out in (i) the NHSmail Acceptable Use Policy and (ii) the local HR policies of the Local Organisation.
Data Protection Officers (DPO)	Kevin Willis Email: nhsdigital.dpo@nhs.net Tel: 0300 303 5678 NHS Digital 1 Trevelyan Square Boar Lane Leeds LS1 6AE			As set out in each Local Organisation's Transparency Notice [Local Organisation] DPO: Email: Address:
Accountability Requirements				
Accountability	✓	NHS Digital, as the National Host Organisation, is the Controller responsible for managing the necessary commercial relations (e.g. with Accenture, the Processor) and also providing funding, technical support, service governance and roll out. In addition to this, it is NHS Digital's responsibility as a controller and primary contracting party with Accenture to approve sub-processors. NHS Digital is therefore responsible for complying with the following provisions of UK GDPR in relation to the operating and maintenance of NHSmail: • Article 5(2) (Accountability) • Article 24 (Responsibility of the Controller) • Article 25 (Data protection by design and default) • Article 28 (Processors)	✓	Through consuming this service, Local Organisations are responsible for ensuring the data their users process through the available capabilities are UK GDPR compliant and also subject to the appropriate internal legal and governance controls. Local Organisations are therefore responsible for complying with the following provisions of UK GDPR in relation to the operating and maintenance of NHSmail: • Article 5(2) (Accountability) • Article 24 (Responsibility of the Controller) • Article 25 (Data protection by design and default) • Article 28 (Processors) • Article 30 (Records of processing activities) • Article 31 (Co-operation with the supervisory authority)

		• Article 30 (Records of processing activities) • Article 31 (Co-operation with the supervisory authority) • Article 32 (Security of processing) • Article 33 (Personal data breach reporting to the ICO) • Article 34 (Personal data breach notification to data subjects) • Article 35 (Data protection impact assessment) • Article 36 (Prior consultation) • Articles 37-39 (DPO) • Articles 44 – 49 (Transfers of personal data to third countries or international organisations)		• Article 32 (Security of processing) • Article 33 (Personal data breach reporting to the ICO) • Article 34 (Personal data breach notification to data subjects) • Article 35 (Data protection impact assessment) • Article 36 (Prior consultation) • Articles 37-39 (DPO) • Articles 44 – 49 (Transfers of personal data to third countries or international organisations)
Compliance with Data Protection Principles				
Article 5 (1)(a) Lawfulness - **personal data** is processed lawfully in relation to the data subject	✓	NHS Digital is responsible for determining the purposes and means for the processing of the personal data in its role as National Host Organisation of the NHSmail service under the 2016 Directions through: • establishing an information system for the collection, analysis, publication and dissemination of personal data about individuals relating to the NHSmail service under the 2016 Directions; • carrying out a system delivery function of the Secretary of State in the operation and delivery of the NHSmail service under the 2016 Directions. The lawful basis for processing the personal data obtained by NHS Digital in relation to its role as National Host Organisation of the NHSmail service, is solely determined by NHS Digital as Article 6(e) (public task).	✓	Local Organisations are responsible for determining the purpose for the capture, use and storage of the personal data processed as part of their management of NHSmail at a local level. As a consumer of the NHSmail service, it is the responsibility of Local Organisations to set out local policies and procedures on how to capture, use, store and, where applicable, share data (including patient identifiable data) at a local level. Further to this, it is the responsibility of the Local Organisation to be transparent to data subjects about what personal data is used/stored and the purposes to which the Local Organisation shall use their data and confirm this through Transparency / Fair Processing Information documents. The lawful basis for processing the personal data obtained by Local Organisations in relation to the NHSmail service is solely determined by each Local Organisation under UK GPDR.
Article 5(1)(a) Lawfulness - **special**	✓	The lawful basis for processing the special categories of personal data processed by NHS Digital in relation to its role as National Host Organisation of the NHSmail service is determined by NHS Digital	✓	The lawful basis for processing the special categories of personal data obtained by a Local Organisation in relation to the NHSmail service is determined by that Local Organisation under UK GDPR.

categories of personal data are processed lawfully in relation to the data subject		as Article 9(2)(h) (management of health or social care systems and services) of UK GDPR, supplemented by paragraph 2 of Part 1, Schedule 1 of the Data Protection Act 2018.		
Article 5(1)(a) and Articles 12-14 - Fairness and transparency - personal data is processed fairly and in a transparent manner in relation to the data subject	✓	NHS Digital is responsible for providing a transparency notice in respect of the personal data it processes as part of maintaining and operating the NHSmail service as the National Host Organisation. It currently achieves this through linking to the relevant Fair Processing / Transparency Information on the NHSmail portal: https://support.nhs.net/article-categories/gdpr-england/	✓	Local Organisations are responsible for providing a transparency notice in respect of the personal data it processes through the NHSmail service. It is the responsibility of Local Organisations to ensure their staff have read and understood how their organisation uses and process personal data. This includes, but is not limited to, ensuring that individuals read: the Acceptable Use Policy for NHSmail and abide by it; local and national policy documents and guidance published regarding NHSmail and Transparency / Fair Processing Information; and briefing data subjects referenced in the use of NHSmail and O365 tools. Further to this, Local Organisations must ensure they put a DPIA in place, provide guidance to their users and publish appropriate privacy information to patients. This information should include data subject rights under the UK GDPR, what personal data is used/stored, the purposes to which the Local Organisation shall use their data and the role of NHS Digital as the National Host Organisation.
Article 5(1)(b) - Purpose limitation - personal data is collected for specified, explicit and legitimate purposes and is not further processed in a manner incompatible with those purposes	✓ ✓	The purposes for the capture, use and storage of the data in relation to its role as the National Host Organisation, are determined by NHS Digital, to the extent set out in the 2016 Directions. In relation to its role as the National Host Organisation, NHS Digital is responsible for ensuring that the personal data is not further processed in a manner incompatible with the overall purposes of the 2016 Directions.	✓ ✓	The purposes for the capture and use of the data are jointly determined by NHS Digital, in its role as the National Host Organisation and the Local Organisations in relation to the data that is processed within NHS Directory. It is the responsibility of Local Organisations to keep the NHS Directory up to date using local data sources. With regard to the capture, use and storage of data within the Local Organisation's use of their local NHSmail system, this is wholly determined by the Local Organisation itself. It is expected that any storage is properly managed in line with a secure local clinical system. Local Organisations are also responsible, at the local level, for ensuring that the personal data is not further processed in a manner incompatible with the overall purposes of data processing in relation to the NHSmail service.

Article 5(1)(c) – Data minimisation - personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed	✓	NHS Digital is responsible for ensuring that the personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed, in relation to its role as the National Host Organisation.	✓	Local Organisations are responsible for ensuring that the personal data processed as part of the NHSmail service at a local level must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
Article 5(1)d) - Accuracy - personal data must be accurate and where necessary kept up to date; reasonable steps must be taken to rectify or erase inaccurate personal data	✓	NHS Digital is responsible for ensuring, in relation to its role as the National Host Organisation, that personal data must be accurate and where necessary kept up to date, and for taking reasonable steps to rectify or erase inaccurate personal data. Due to the fact that NHSmail manages high volumes of data across the service, NHS Digital relies on Local Organisations to keep records up to date at a local level.	✓	Local Organisations are responsible for ensuring, in relation to use of the NHSmail service at a local level, that the personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This is especially pertinent in relation to: • Personal data – can be edited by Local Organisations, to ensure records are kept current. • NHS Directory - Local Organisations are responsible for populating user information in NHS Directory, as well as maintaining and deleting contact details held on the NHSmail directory, which feeds into the national NHS Directory. • Email, video conferencing and other collaboration data – data quality of content sent over email or video conferencing capabilities is responsibility of users at local level.
Article 5(1)(e) - Storage limitation - personal data must be kept in identifiable form for no longer than necessary for the purpose for which the	✓	NHS Digital is responsible for ensuring, in relation to its role as the National Host Organisation, that personal data must be kept in an identifiable form for no longer than necessary for the purpose for which the personal data are processed. As the National Host Organisation, NHS Digital is responsible for publishing the NHSmail Data Retention and Information Management Policy which sets out the data storage periods for the service and the minimum retention periods for which the data will be kept.	✓	Local Organisations are responsible for ensuring that personal data at the local level must be kept in identifiable form for no longer than necessary for the purpose for which the personal data are processed. Local Organisations can align to the agreed national processes as set out in NHS Digital's Data Retention and Information Management Policy. If Local Organisations wish to store data beyond the agreed national minimum, then they are expected to also have their own local policies, procedures and technical measures in place to facilitate this.

personal data are processed				It is also a responsibility of Local Organisations to brief their staff members in the use of NHSmail and O365 tools, and how storage limitations should apply to these tools. 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 Organisation transparency information must be updated to record how this data is captured and stored.
Article 5(1)(f) - (Integrity and confidentiality - personal data will be processed in a manner that ensures appropriate security including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage	✓	NHS Digital is responsible for ensuring, in relation to its role as the National Host Organisation, that personal data will be processed in a manner that ensures appropriate security including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. NHSmail is accredited to the NHS secure email standard (DCB1596). It is the responsibility of NHS Digital to secure annual accreditation to this standard. It is a responsibility of NHS Digital to publish guidance for Local Administrators on how to operate in their role within the NHSmail service. This shall be provided through the NHSmail support site, monthly webinars and bulletins.	✓	Local Organisations are responsible for ensuring, in relation to use of NHSmail at a local level, that personal data will be processed in a manner that ensures appropriate security including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. Local Organisations are also responsible for determining any additional Office 365 applications O365 NHSmail Portal Management – Getting Started Guide – NHSmail Support they would like to enable at a local level. This is on the basis that they have carried out the appropriate security based risk assessment for use of the application at that local level, including any international data transfer requirements. Local Organisations shall either: (i) appoint Local Administrators to manage and maintain the NHSmail service for that organisation at a local level including the adding, removal and suspension of NHSmail accounts; or (ii) Appoint shared mailbox owners (privacy officers) to oversee the IG and data management for their site. These arrangements are typically for smaller organisations that (a) utilise the National Administration Service (NAS) provided by Accenture (through contract with NHS Digital as Joint Controller), or (b) appoint a Local Sponsoring Organisations (e.g. clinical commissioning group) to provide the administration and maintenance of the email accounts and collaboration tools). Local Organisations using APIs to extract personal data or official data from the NHSmail service are required to protect and secure the data via their local processing standards and policies. It is the responsibility of Local Organisations to complete an annual Data Security and Compliance Toolkit to ensure that their NHSmail users have completed information governance training. Local Organisations will need to ensure all assertions and mandatory evidence items are complete and up to date at all times.

				New organisations joining NHSmail are required to self-declare information governance compliance before NHSmail accounts are authorised.
Data Subjects' Rights and Contact Details				
Article 12 – Transparent information, communication and modalities for the exercise of the rights of the data subject	✓	NHS Digital is responsible for compliance with the obligations in Article 12 in relation to the processing of all personal data to the extent it has obtained through the provision of the NHSmail service as National Host Organisation. Through its Transparency / Fair Processing notice, NHS Digital sets out what rights under UK GDPR are available in relation to this service and how to exercise those rights. NHS Digital publishes its Transparency / Fair Processing Information and Further Information on GDPR here: https://support.nhs.net/article-categories/gdpr-england/	✓	Local Organisations are responsible for compliance with the obligations in Article 12 in relation to the processing of all personal data to the extent it processes through the provision of the NHSmail service at a local level. The Local Organisation should set out this information in its own Transparency / Fair Processing notice that it provides to local level users in relation to its operation / management of that service.
Article 13 – Information to be provided where personal data are collected from the data subject	✓	NHS Digital is responsible for providing data subjects with the information required in Article 13 in relation to the processing of all personal data to the extent it has obtained through the provision of the NHSmail service at National Host Organisation. NHS Digital publishes its Transparency / Fair Processing Information and Further Information on GDPR here: https://support.nhs.net/article-categories/gdpr-england/	✓	Local Organisations are responsible for providing data subjects with the information required in Article 13 in relation to the processing of all personal data to the extent it has obtained through the provision of the NHSmail service at local level. For NHSmail use by NHS Digital as a Local Organisation, this Transparency / Fair Processing Information is available here: https://digital.nhs.uk/about-nhs-digital/our-work/keeping-patient-data-safe/gdpr/gdpr-register/nhsmail-use-by-nhs-digital
Article 14 – Information to be provided where personal data has not been obtained from the data subject	✓	NHS Digital is responsible for providing data subjects with the information required in Article 14 in relation to the processing of all personal data to the extent it has obtained through the provision of the NHSmail service other than from the data subject, as National Host Organisation.	✓	Local Organisations are responsible for providing data subjects with the information required in Article 14 in relation to the processing of all personal data, through the provision of the NHSmail service at a local level and is collected from sources other than the data subject
Article 15 - Data subject access request	✓	NHS Digital is responsible for compliance with data subject access requests regarding the processing of personal data to the extent it has obtained that data through the provision of the NHSmail service as National Host Organisation.	✓	Local Organisations are responsible for compliance with data subject access requests regarding the processing of personal data to the extent it has processed through the provision of the NHSmail service at local level.

		NHSmail 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. With regard to the national processes, NHSmail provide the infrastructure and system for Local Organisations to access data but it is the responsibility of Local Organisations to initiate and conduct searches for their own purposes. This is set out in the 'Ways of accessing data' section of the NHSmail Data Retention and Information Management Policy and the Access to Data Procedure. It is the responsibility of NHS Digital to only facilitate requests from the Local Administrator at the relevant Local Organisation, providing that the Local Administrator follows the guidance in the Access to Data Procedure document. Once the request is fulfilled, the requesting Local Organisation will take ownership of the data that is received from the NHSmail Live Service team. For the avoidance of doubt NHS Digital or Accenture are not responsible for the requested data once it has been sent.		Requests should be made to the NHSmail Local Administrator within the Local Organisation that owns the requesting user's NHSmail account following agreed local and national processes. It is the responsibility of the Local Organisation to answer data subjects' right of access requests using information available on their local system in the first instance. If further data is required to meet this request that the Local Organisation may not readily have access to, then the NHSmail Data Retention and Information Management Policy and the Access to Data Procedure provides a framework for accessing data that might be required in a 'forensic investigation'. It is the responsibility of the Local Organisation to ensure investigation requests are submitted from the Local Administrator of that organisation and are authorised by the correct approver depending on the organisation type, as set out in the Access to Data Procedure policy. It is the responsibility of the Local Organisation to take ownership of the data that is received from the NHS Live Service team from this request process. On receipt of the data, the organisation must ensure it is stored securely and managed in accordance with local information governance policy and data protection legislation.
Articles 16 – 22 - Other applicable data subject rights	✓	NHS Digital is responsible for complying with the exercise of any other data subject rights regarding the processing of personal data to the extent it has obtained that personal data through the provision of the NHSmail service as National Host Organisation. In this vein, NHS Digital is reliant on Local Organisations to keep local data sources up to date and reflected within the NHS Directory. Where there is a technical requirement to comply with the data subject rights request because the Local Organisation cannot carry this out, NHS Digital will support the Local Organisation with that request. <u>Right to rectification</u> It is the responsibility of NHS Digital to support Local Organisations to rectify any incorrect or incomplete recorded personal details in the NHSmail service, including the NHS Directory, where requested from a Local Organisation's Local Administrator or from an NHSmail user through the NHSmail Help-desk who can make the necessary amendments. <u>Right to restrict processing</u>	✓	Local Organisations are ultimately responsible for compliance with data subject rights requests regarding the processing of personal data to the extent it has processed through the provision of the NHSmail service at local level. Local Organisations are responsible as the local data source for NHSmail, and in particular NHS Directory, to keep personal data up to date. <u>Right to rectification</u> It is the responsibility of Local Organisations through their Local Administrators to support data subjects in making the necessary amendments where their personal data may be incomplete or incorrect. Local Organisations have full access to the NHS Directory, and it should be regarded as the single source of truth for users in the NHSmail system nationally. NHS Digital relies on Local Organisations as the local data source in relation to data subjects which are managed under each respective local use of the service. Further, it is the responsibility of Local Organisations to ensure that the personal data of data subjects is correct.

		It is the responsibility of the NHS Digital NHSmail Live Service team to support Local Organisations where they receive a request to restrict processing of data where a request to rectify accuracy is received. A request to restrict processing may be received from a Local Organisation's Local Administrator or from an NHSmail user through the NHSmail Help-desk who can then apply the necessary restrictions. Right to object It is the responsibility of NHS Digital to support Local Organisations with a request from a data subject to stop processing data where there are legitimate grounds to do so. The NHSmail Live Service manages high volumes of data across the service, therefore it is reliant on Local Organisations to have their own policies and procedures in place to ensure that the NHSmail Live Service contains up to date and correct information. This allows NHS Digital to respond to any requests of this type it receives as the National Host Organisation. Right not to be subject to a decision based solely on automatic processing As a data controller, it is the responsibility of NHS Digital as the National Host Organisation of NHSmail to not subject data subjects to a decision based solely on automatic processing where a request is received. There is currently limited scope within the NHSmail service for NHS Digital to subject data subjects to a decision based solely on automatic processing in its role as the National Host Organisation. This section will be reviewed in the event that this functionality is developed.		Right to restrict processing It is the responsibility of Local Organisations through their Local Administrators to support data subjects in exercising this right. In responding to a request to apply this right, a Local Organisation through its Local Administrator may submit a request to hide an individual from the NHS Directory. To process this request, NHS Digital requires permission from account owner or the Local Organisation HR director (or equivalent). The request should be forwarded to the NHSmail Live Service team (NHS Digital) via feedback@nhs.net before the NHSmail helpdesk (Accenture) can action. Local Organisations have full access to the NHS Directory, and it should be regarded as the single source of truth for users in the NHSmail system nationally. NHS Digital relies on Local Organisations as the local data source in relation to data subjects which are managed under each respective local use of the service. It is the responsibility of Local Organisations to ensure that the personal data of data subjects is dealt with as the data subject requests, within the scope of their available legal rights. Right to object It is the responsibility of Local Organisations through their Local Administrators to support data subjects in exercising this right. It is expected that Local Organisations through their Local Administrators are able to exercise this right on behalf of the data subjects within the NHS Directory functionality available to them. Local Organisations have full access to the NHS Directory and it should be regarded as the single source of truth for users in the NHSmail system nationally. NHS Digital relies on Local Organisations as the local data source in relation to data subjects which are managed under each respective local use of the service. It is the responsibility of Local Organisations to ensure that the personal data of data subjects is dealt with as the data subject requests, within their legal rights. Right not to be subject to a decision based solely on automatic processing

				It is the responsibility of Local Organisations through their Local Administrators to support NHSmail users in exercising this right. Local Organisations may integrate their local use of NHSmail with a patient system that subjects data subjects to automated decision making. In this instance, it is the responsibility of that Local Organisation to manage that integration and ensure that data subjects have a choice as to whether a decision is made about them manually where automated decision making occurs. Each Local Organisation should have their own local policy to cover when a data subject exercises this right. This policy should be read and understood by relevant staff members.
Complaints	✓	NHS Digital as a controller processing personal data is responsible for investigating any complaints regarding the processing of personal data it has obtained through the provision of the NHSmail service it holds as the National Host Organisation. NHS Digital in its role as National Host Organisation may provide assistance to Local Organisations to investigate any complaints, if such help is required.	✓	Local Organisations in their role as controller processing personal data are responsible for investigating any complaints regarding the processing of personal data they have processed through the provision of the NHSmail service at local level
Contact Point for Data Subjects	✓	NHS Digital is the contact point for Data Subjects referred to in its Transparency Notice / Information in relation to any processing of personal data through the provision of the NHSmail service as the National Host Organisation.	✓	Local Organisations are the contact point for Data Subjects referred to their Transparency Notice / Information in relation to any processing of personal data through the provision of the NHSmail service at local level If Local Organisations receive a technical enquiry about the NHSmail service or its infrastructure, then they can raise a ticket with the NHSmail helpdesk to be assigned a ticket reference via the process outlined at https://support.nhs.net/knowledge-base/complaints-and-escalations-process/ If Local Organisations receive a query related to information governance or NHSmail process more generally and they are unable to answer this in the first instance then they should contact NHS Digital for support via the Contact Centre at enquiries@nhsdigital.nhs.uk or the NHSmail live service team directly at feedback@nhs.net.
Personal Data Breach and notifications				
Article 33-34 – Notification of personal data	✓	NHS Digital shall be responsible for putting in place appropriate policies for detecting and preventing actual and potential personal	✓	Local Organisations shall be responsible for putting in place appropriate policies for detecting and preventing actual and potential personal data

breach to supervisory authority/data subject		data breaches where those breaches impact the national NHSmail system. NHS Digital has internal operational processes in place for dealing with data breaches, with support from its internal Data Security Centre, that will be invoked in the event of breach. In the event of a breach that impacts the NHSmail service as a whole, it is the responsibility of NHS Digital to investigate breaches, to comply with the relevant reporting obligations and to notify Local Organisations with details of the breach. NHS Digital shall determine any subsequent reporting of any Personal Data Breach to a Supervisory Authority or (where applicable) notification to Data Subjects shall be undertaken by NHS Digital.		breaches at as they occur at the local level under the Local Organisation's jurisdiction. In absence of any provision to the contrary, Local Organisations will also be responsible to report a Personal Data Breach (where the breach occurs under the Local Organisation's jurisdiction) to a Supervisory Authority or (where applicable) notification to Data Subjects shall be undertaken by the Local Organisation
Data Protection Impact Assessment				
Articles 35-36 – Data Protection Impact Assessment and prior consultation.	✓	NHS Digital is responsible for ensuring a data protection impact assessment is in place for the NHSmail service in its role as the National Host Organisation. NHS Digital publishes a data protection impact assessment to support Local Organisations with the completion of their local documentation and guidance for compliance with data protection obligations at a local level.	✓	Local Organisations are responsible for ensuring a data protection impact assessment is in place at the local level, as part of their wider responsibility of ensuring the data their users use and store is compliant with data protection laws as well as the appropriate internal legal and governance controls.