



The DBTH Subject Access Request (SARs & DSARs) Policy

This is a new Policy



Did you print this document yourself?

The Trust discourages the retention of hard copies of policies and can only guarantee that the policy on the Trust website is the most up-to-date version. **If, for exceptional reasons, you need to print a policy off, it is only valid for 24 hours.**

Executive Sponsor(s):	Dan Howard Chief Information officer (CIO) & Senior Information Risk Owner (SIRO)
Authors (this version)	Roy Underwood – Information Governance Manager David Linacre – Head of Digital Anthony Jones – Deputy Director of HR Rhona McCleery – Information Governance Manager
Date written/revised:	February 2024
Approved by:	The Information Governance Committee
Date of approval:	20 th May 2024
Date issued:	October 2024
Next review date:	May 2027
Target audience:	Trust-wide

Amendment Form

Version	Date Issued	Brief Summary of Changes	Author
1	October 2024	This is a new procedural document please read in full	Roy Underwood – Information Governance Manager David Linacre – Head of Digital Anthony Jones – Deputy Director of HR Rhona McCleery – Information Governance Manager

Contents

	Page No.
1 INTRODUCTION	4
2 PURPOSE	4
3 SCOPE	5
4 DUTIES AND RESPONSIBILITIES	6
5 PROCEDURE	7
5.1 Qualified Not Absolute Rights.....	10
5.2 Transparency and Modalities	10
5.3 Notification Obligation.....	10
5.4 Recognising Individual Rights Requests.....	10
5.5 Fees and Refusal of Requests	11
5.6 Response Times	11
5.7 Verifying Identity	12
5.8 Information to be Provided to Requesters within the First 30 Days	12
5.9 Scope of Requests.....	13
5.10 Third Party Requests.....	13
6 TRAINING/SUPPORT	13
7 MONITORING COMPLIANCE WITH THE PROCEDURAL DOCUMENT	14
8 DEFINITIONS	14
9 EQUALITY IMPACT ASSESSMENT	15
10 ASSOCIATED TRUST & LEGAL DOCUMENTS	15
10 DATA PROTECTION.....	16
11 REFERENCES	16
12 APPENDICES	17
13 EQUALITY IMPACT ASSESSMENT - PART 1 INITIAL SCREENING	37

1 INTRODUCTION

Individuals have a right to apply for access to health information held about them and, under the correct circumstances, this can also apply to requesting information about other people, or a deceased person. All NHS organisations must ensure they have adequate procedures in place to enable people to exercise this right. This also applies to staff members who wish to access their staff records.

The main legislative measures that give rights of access to health records include:

- The Data Protection Act 2018 (DPA) / The UK General Data Protection Regulations (UK GDPR 2021) - rights for living individuals to access their own records. The right can also be exercised by an authorised representative on the individual's behalf.
- The Access to Health Records Act (AHRA) 1990 - rights of access to deceased patients' health records by specified persons.
- Individuals Rights - One of the aims of the General Data Protection Regulation (UK GDPR) is to empower individuals and give them control over their personal data. This includes the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object and the right not to be subject to a decision based solely on automated processing.
- The Medical Reports Act (MRA) 1988 - rights for individuals to have access to reports, relating to them, provided by medical practitioners for employment or insurance purposes.

2 PURPOSE

A Subject Access Request (SAR) can be received by anyone within the Trust.

Upon receipt of a SAR, this MUST be copied to the Information Governance, Caldicott & SIRO Support Team (IGC&SST) via: dbth.dpo@nhs.net immediately, for them to ensure correct action and progress by the appropriate **Divisional or Corporate General Manager**, as they are likely to be the focus of the applicant's request for data.

The IGC&SST will record all requests however, it is NOT their job to service any Patient Subject Access Requests (SARs) or Staff Data Subject Access Requests (DSARs) however, along with P&OD Human Resources staff, they will always provide best assistance and focus concerning methodology and deadline management.

The UK GDPR 2021, the Data Protection Act 2018 (DPA 2018), and the Access to Health Records Act 1990 (AHRA) state that Trusts have **one calendar month** to comply with requests. They can ask for an increase in the time allowance – up to 90 days – where the application is complex and excessive. There is ICO advice to enter dialogue with the

applicant to get more focus and a more limited scope in order that the task is 'reasonable' for a public authority to attend to.

Failing to comply with this requirement may carry financial penalties for the Trust, as failure to comply with a request for subject access, without valid justification, is treated as a serious matter and may be referred to the ICO. Such complaints are dealt with as a matter of priority and may lead to a full-scale investigation into an organisation's procedures and practices. Fees for access to health records may be requested in some cases and must be paid in advance of the records being dispatched.

Within this policy is further information as to how a SAR is handled, to ensure that it is done correctly, securely, and efficiently.

3 SCOPE

The scope of this Policy is to ensure that:

- The Trust is compliant with the UK GDPR 2018 and the DPA 2018, where there is a one calendar month target to release personal health information from the date of receipt of a valid Subject Access Request (SAR) including a Data Subject Access Request (DSAR) which the Trust labels for any SAR that is requesting personal data that is not of a clinical nature.
- The Trust has clear lines of accountability for the monitoring and completion of SARs and DSARs within the specified target.
- All services responsible for supporting the completion of SARs and DSARs within the one calendar month target are aware of their responsibilities towards, and are supportive of the Trust's obligation to meet, the access to health records target.

This Policy applies to all those working for the Trust in whatever capacity, including the Trust's staff, volunteers, students, temporary workers, contractors, suppliers and Third Parties. It also applies to Third Party providers who may hold Information belonging to the Trust, including patient information.

This document applies to and is relevant across all services/departments.

4 DUTIES AND RESPONSIBILITIES

Persons with lead responsibility for this policy are:

Chief Executive

The Chief Executive has overall accountability for ensuring that all laws are implemented within the Trust including the UKUK GDPR 2021, the DPA 2018, the AHRA 1990, and the MRA 1988. In addition, the Chief Executive has overall accountability for implementing records management within the Trust.

Divisional / Corporate Managers

All DSARs received from an individual as the applicant will be passed to the appropriate Divisional/Corporate Manager with the opportunity – from the policy - for utilising a Task & Finish approach.

Senior Information Risk Owner (SIRO)

The Trust SIRO is accountable for information risk throughout the organisation.

Caldicott Guardian

The Trust Caldicott Guardian is responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing.

Data Protection Officer (DPO)

The DPO will assist in monitoring internal compliance, inform and advise on data protection obligations, and act as a contact point for data subjects and the supervisory authority (Information Commissioners Office – ICO).

Information Asset Owners (IAOs)

IAOs are responsible for information assets which include health records within each service. It is the IAO's responsibility to make sure that staff within Service areas follow the outlined procedures to ensure the Trust is compliant with appropriate laws.

Medical Records Casenote Release Team

Requests for Medical Casenotes under a SAR received by the Trust are dealt with by the Medical Records Casenote Release Team at the Trust for review and response. All request details will be entered into a log and this will be maintained to monitor compliance to ensure all requests are answered in a timely manner. Prior to the release of any information, the Medical Records Casenote Release Team must be satisfied as to the identity of the person making the request. No information will be released until this identification has taken place. Appendix A details the process flow.

People & Organisational Development

The P&OD Team will provide assistance and support to Divisional and Corporate Management Teams as and when required, particularly in such instances where there is an ongoing HR process

Information Governance Manager

Will assist and liaise with Divisional and Corporate General Managers as they service their DSAR tasks within the legal deadlines.

5 PROCEDURE

The preferred format for submitting SARs by an individual would be in electronic form i.e. email or similar however applicants may submit their request in writing if they prefer. Electronic applications help to ensure that all the information required to effectively process the request is in one place. However, the Trust recognises that a request may be in any format - verbal, email, social media, written etc.

Therefore, as in [Appendix A](#):

In the case of Patient SARs as **managed by Medical Records/Casenote Release Department**:

- The request shall be logged and managed through a secure register.
- The request should be acknowledged by the Trust upon receipt.
- The identity of the individual making the request shall be verified.
- No charge shall be applied – other than in exceptional circumstances described in the section 'Fees and Refusal of Requests'.
- Trust systems and records shall be searched to identify the information held.
- Information shall be prepared and not re-processed to create any new records.
- Information shall be provided in written or electronic formats, with the NHS Secure EGRESS platform being the Trusts' preferred option.
- If the Trust agrees that information held is inaccurate, the Trust shall update their current information.

In the case of Staff DSARs:

- The process will follow as for Patient SARs but **managed via the Divisional General Managers**.
- A record of Staff DSARs will be held by the IG, Caldicott and SIRO support (IGC&SS) team.
- A copy of the completed Task and Finish log should be sent to the IGC&SS at dbth.dpo@nhs.net immediately on completion of the request (a copy of the response is not required but the log should detail all action taken and include dates).

The Trust should provide the information in a timely manner. In most circumstances, information requests should be provided within one calendar month from the date of initial receipt. If a request is complex or if multiple SARs are made by the same individual, then the

response time may be extended by a further two months. If this is the case, the Trust expects the individual to be advised with the appropriate explanation for the extension.

The Trust shall provide its response in a concise, transparent, and accessible manner using clear and plain language (as per ICO instruction – the response should be capable of being understood by the average person, or where appropriate, a child).

All managers and staff must comply with any request for personal data forwarded to them by the Medical Records Casenote Release Team or the Divisional General Manager as quickly as possible, and that will generally be within 1 month plus 1 day from the date of receipt of the application with day 1 being the day after the date of receipt in order that the Trust has the full 30 days to service the request.

Data Subjects' Rights

The rights of data subjects under which individuals may make requests include the following:

- Right to Access
- Right to Rectification
- Right to Erasure
- Right to Restriction
- Right to Data Portability
- Right to Object
- Rights related to Automated Decision Making and Profiling

In addition to the above, data subjects also have the right to be informed. The Trust fulfils this by providing details of its Privacy Notices whenever it collects personal data about individuals.

<https://www.dbth.nhs.uk/wp-content/uploads/2021/10/Full-Privacy-notice-for-website.pdf>

Rights of Others:

RESTRICTION BASED ON ARTICLE 23(1): PROTECTION OF RIGHTS OF OTHERS

<https://www.legislation.gov.uk/ukpga/2018/12/schedule/2/part/3/enacted>

16 The protection of the rights of others: general

- (1) Article 15 (1) to (3) of the GDPR (confirmation of processing, access to data and safeguards for third country transfers), and Article 5 of the GDPR so far as its provisions correspond to the rights and obligations provided for in Article 15(1) to (3), do not oblige a controller to disclose information to the data subject to the extent that doing so would involve disclosing information relating to another individual who can be identified from the information.

- (2) Sub-paragraph (1) does not remove the controller's obligation where
- (a) The other individual has consented to the disclosure of the information to the data subject,
 - (b) It is reasonable to disclose the information to the data subject without the consent of the other individual.
- (3) In determining whether it is reasonable to disclose the information without consent, the controller must have regard to all the relevant circumstances, including
- (a) The type of information that would be disclosed,
 - (b) Any duty of confidentiality owed to the other individual,
 - (c) Any steps taken by the controller with a view to seeking the consent of the other individual,
 - (d) Whether the other individual is capable of giving consent, and
 - (e) Any express refusal of consent by the other individual.
- (4) For the purposes of this paragraph
- (a) "Information relating to another individual" includes information identifying the other individual as the source of information;
 - (b) An individual can be identified from information to be provided to a data subject by a controller if the individual can be identified from—
 - (i) That information, or
 - (ii) That information and any other information that the controller reasonably believes the data subject is likely to possess or obtain.

17 Assumption of reasonableness for **health workers**, social workers and education workers

- (1) For the purposes of paragraph 16(2)(b), it is to be considered reasonable for a controller to disclose information to a data subject without the consent of the other individual where
- (a) The health data test is met,
 - (b) The social work data test is met, or
 - (c) The education data test is met.
- (2) The **health data test is met if**
- (a) The information in question is **contained in a health record, and**
 - (b) **the other individual is a health professional** who has compiled or contributed to the health record or who, in his or her capacity as a health professional, **has been involved in the diagnosis, care or treatment of the data subject.**

In other words, **non-health professionals names** in digital or manual records **do not meet** the health data test.

5.1 Qualified Not Absolute Rights

All of the rights listed above are qualified rights, meaning there are some exceptions to when they must be applied. Whilst the Trust must always acknowledge a request has been made, there may be legal grounds for not complying with it. In this case, the requester will be made aware.

5.2 Transparency and Modalities

When dealing with individual rights requests, the Trust will consider the UK GDPR concepts of transparency and modalities. These are responsibilities on Data Controllers in terms of how they ensure data subjects' rights are facilitated. Specifically, information in connection to data subjects' rights should be provided to data subjects in a 'concise', transparent, intelligible and easily accessible form', 'using clear and plain' language (transparency). In addition, information should be provided in any form as per the requirements of the data subject, this can include all written forms, hard copy or electronic and in certain cases oral provision of information (modalities).

5.3 Notification Obligation

When processing individual rights requests around the right to erasure, rectification and restriction, the Trust will also consider the 'notification obligation' conferred by Article 19 of the UK GDPR. This means that when the Trust actions a request around one of the above rights, we are obligated to communicate what we have done to any other controllers of processors whom we have shared the data with previously, except where this is impossible or involves disproportionate effort.

5.4 Recognising Individual Rights Requests

Who can make a Request?

- The individual themselves (Patient, service User or Staff Member)
- Individuals requesting access on behalf of a child for whom they have parental responsibility
- A representative nominated by the individual to act their behalf such as solicitors or a relative, where there is valid consent by the individual granting this authority
- In certain situations, a person granted an attorney or agent by the Court of Protection on behalf of an adult who is incapable of consent

Key Points:

- A request can be made verbally or in writing.
- A request can be made to any part of the organisation and does not have to be to a specific person or contact point.
- A request does not need to mention the phrase containing the right being exercised or the relevant UK GDPR Article to be a valid request. As long as the individual has clearly described their request; this is valid. We will check with the requester that we have understood their request and request any identification / authorisation (if required).
- We will record the details of all requests we receive.

The format that an individual rights request is received may differ from request to request. Therefore, if an individual writes to the Trust or speaks to the Trust and asks for access, changes, or makes any objections of any kind to the personal data the Trust is processing about them (whether perceived or actual processing of their data) it should be considered and handled where appropriate as an individual rights request.

5.5 Fees and Refusal of Requests

Individual rights requests are generally free of charge. However, if the Trust considers that a request is 'manifestly unfounded' or excessive (repeated) we can:

- request a 'reasonable fee' to deal with the request; or
- refuse to deal with the request

In either case the Trust will need to document and justify the decision and let the requestor know about the decision as soon as possible.

A reasonable fee should be based on the administrative costs of complying with the request. The Trust does not need to comply with the request until it has received the fee.

5.6 Response Times

Under data protection legislation the Trust has one calendar month to respond to any request. The Trust is implementing this period in line with ICO guidance.

The Trust will calculate the time limit from the day after we receive the request (whether the day after is a working day or not) until the corresponding date 30 days from that point (Public Holidays are excluded).

Extending the response time: The Trust can extend the time to respond by a further two months if the request is complex or we have received a number of requests from an individual. We will let the individual know without undue delay and within one month of receiving their request and explain why the extension is necessary. The decision to extend should only be done in consultation with the Trust DPO.

However, it is the ICO's view that it is unlikely to be reasonable to extend the time limit if:

- The request is manifestly unfounded or excessive.
- An exemption applies; or we are requesting proof of identity before considering the request.

5.7 Verifying Identity

If the Trust has doubts about the identity of the person making the request, we can ask for more information. However, it is important that we only request information that is necessary to confirm who they are. We will take into account what data we hold, the nature of the data, and what we are using it for.

We will let the individual know without undue delay that we need more information from them to confirm their identity. We do not need to comply with the request until we have received the additional information.

5.8 Information to be Provided to Requesters within the First 30 Days

If the Trust **is not able to comply** with the request, then the applicant should be advised accordingly and as soon as possible: **in this eventuality, please discuss / seek advice immediately from the DPO: dbth.dpo@nhs.net**

- the reasons we are not taking action.
- their right to make a complaint to the ICO.
their ability to seek to enforce a right through a judicial remedy

If the Trust **is able** to action the request dependent on further information:

- that we are requesting a reasonable fee, or
- that we need additional information to identify the individual

If the Trust **is actioning** the request:

- respond to the request, or
- notify the requestor that we need to extend the response time (up to a further two months – 60/90 days)

5.9 Scope of Requests

Any personal data in relation to an individual, no matter what format, where or how it is stored by the Trust could fall into the scope of an individual rights request.

5.10 Third Party Requests

This request is made under Schedule 2 Part 1 Paragraph 2 and Part 3 (law enforcement) of the Data Protection Act 2018 and the UK GDPR Article 6 (1) (d). Part 3 only applies to competent authorities processing for law enforcement purposes. Therefore, it applies, but is not limited, to:

- the police, criminal courts, prisons, non-policing law enforcement; and
- any other body that has statutory functions to exercise public authority or public powers for any of the law enforcement purposes.
- the key thing to consider is your primary purpose for the processing. This should help you identify whether the processing falls under the UK GDPR rules or satisfies the criteria of the law enforcement purposes under Part 3 of the DPA 2018.
- The law enforcement purposes are defined under section 31 of the DPA 2018 as: ‘The prevention, investigation detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.’

6 TRAINING/SUPPORT

Staff groups requiring training	How often should this be undertaken	Length of training	Delivery method	Training delivered by whom	Where are the records of attendance held?
All Staff – Data Security and Awareness (IG) Training	Upon Commencement of employment and annually thereafter	1 ½ hours	E-learning	Via ESR	ESR

7 MONITORING COMPLIANCE WITH THE PROCEDURAL DOCUMENT

Monitoring the effectiveness of the policy will be achieved through periodic audit with the results going to the Information Governance Committee and then onward to the Finance & Audit Committee for the Board of Directors attention as necessary.

Any serious risks identified will be reported to the Information Governance Committee for awareness.

What is being Monitored	Who will carry out the Monitoring	How often	How Reviewed/ Where Reported to
The Number of DSARs	The IGC&SS Team	6 monthly	IG Committee
The Nature of the DSARs			

8 DEFINITIONS

For the purposes of this document the following definitions apply:

Item	Definition
Access control	The prevention of unauthorised use of a resource, including the prevention of use of a resource in an unauthorised manner.
Asset owner	Individual or organisation having responsibility for specified information asset(s) and for the maintenance of appropriate security measures.
Audit trail	Data collected and potentially used to facilitate any reconstruction of events within the system.
Availability	Information is delivered to the right person, when it is needed.
Confidentiality	Data access is confined to those with specified authority to view the data.
Impact	The embarrassment, harm, financial loss, legal or other damage which could occur in consequence of a particular security breach.
Integrity	All system assets are operating correctly according to specification and in the way that the current user believes them to be operating
Security breach	Any event that has, or could have, resulted in loss or damage to NHS assets, or an action that is in breach of NHS security procedures.
Threat	An action or event that might prejudice security.

9 EQUALITY IMPACT ASSESSMENT

The Trust aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are disadvantaged over others. Our objectives and responsibilities relating to equality and diversity are outlined within our equality schemes. When considering the needs and assessing the impact of a procedural document any discriminatory factors must be identified.

An Equality Impact Assessment (EIA) has been conducted on this procedural document in line with the principles of the Equality Analysis Policy (CORP/EMP 27) and the Equality Diversity and Inclusion Policy (CORP/EMP 59).

The purpose of the EIA is to minimise and if possible remove any disproportionate impact on employees on the grounds of race, sex, disability, age, sexual orientation or religious belief. No detriment was identified. (See Appendix 1).

10 ASSOCIATED TRUST & LEGAL DOCUMENTS

. LINKS TO ANY ASSOCIATED DOCUMENTS

- [Information Governance Policy](#)
- [Records Management Policy](#)
- [Complaints, Concerns, Comments and Compliments Resolution and Learning](#)

Legislation

All staff are required to comply with Data Protection Legislation. This includes:

- [the UK General Data Protection Regulation 2021 \(UK GDPR\)](#)
- [the Data Protection Act \(DPA\) 2018](#)
- [the Law Enforcement Directive](#) (Directive (EU) 2016/680) (LED) and any applicable national Laws implementing them as amended from time to time.

In addition, consideration will also be given to all applicable Law concerning privacy confidentiality, the processing and sharing of personal data including:

- [the Human Rights Act 1998](#)
- [the Health and Social Care Act 2012 as amended by the Health and Social Care \(Safety and Quality\) Act 2015](#)
- [the Common Law Duty of Confidentiality](#)
- [the Privacy and Electronic Communications \(EC Directive\) Regulations](#)

Consideration must also be given to the:

- [Electronic Communications Act 2000](#)
- [Freedom of Information Act 2000](#)

- [Other relevant Health and Social Care Acts](#)
- [Access to Health Records Act 1990](#)
- [SARs Q&A for employers - ICO](#)

11 DATA PROTECTION

Any personal data processing associated with this policy will be carried out under 'Current data protection legislation' as in the Data Protection Act 2018 and the UK General Data Protection Regulation (GDPR) 2021.

For further information on data processing carried out by the trust, please refer to our Privacy Notices and other information which you can find on the trust website:
<https://www.dbth.nhs.uk/about-us/our-publications/information-governance/>

12 REFERENCES

All staff members are required to comply in particular with the provision of the following legislation and Department of Health guidance:

- The Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR) 2021
- The Computer Misuse Act 1990

Other References

- [Trust's Policies and Procedures](#)
- [Data Protection Act 2018](#)
- [ICO Guide to UK GDPR](#)
- [Medical Reports Act 1988](#)
- [National Data Guardian](#)

13 APPENDICES

Appendix A – Requests for Information – Process Flow

Appendix B – Links with more Information on Individual Rights

Appendix C – Application for Access to Health Records

Appendix D – Application for Access to Records – Member of Staff

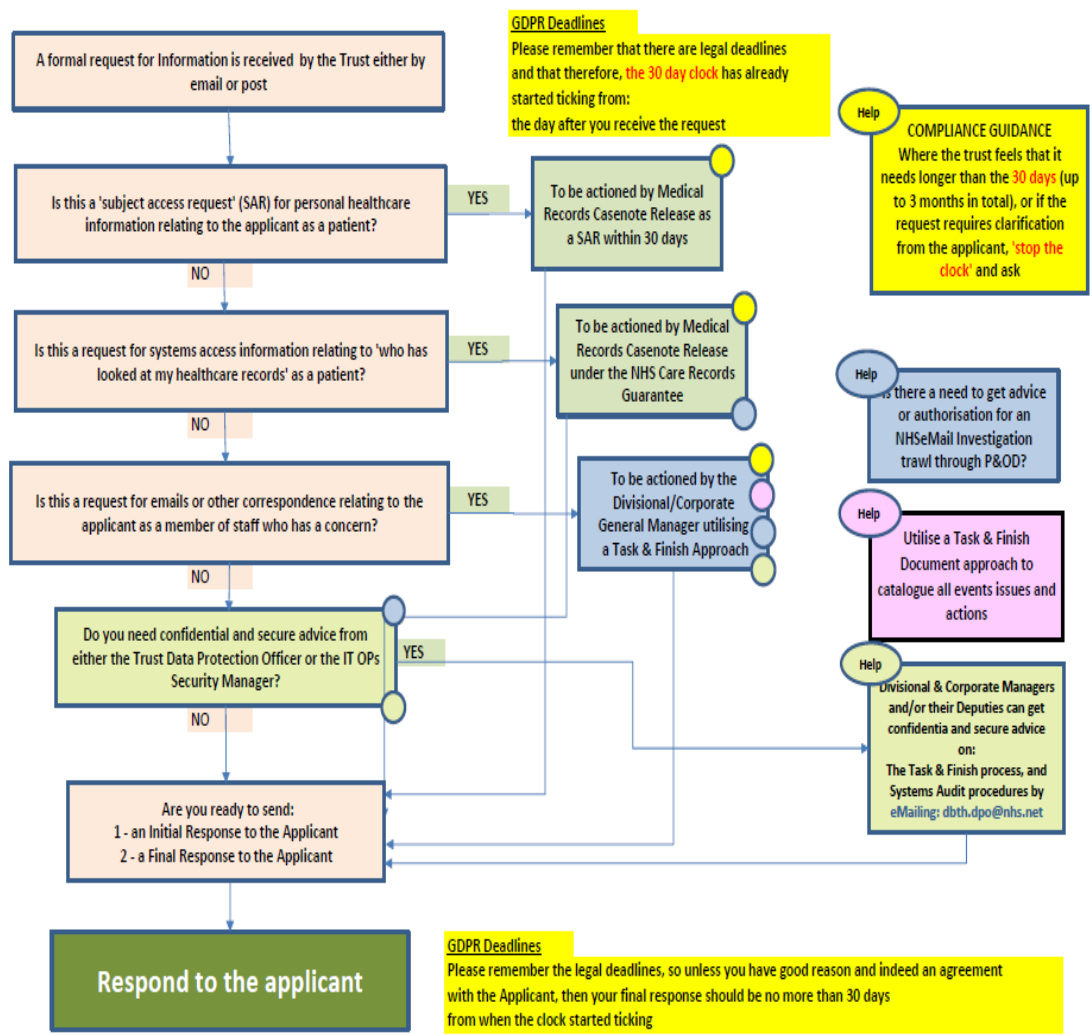
Appendix E – Task and Finish template - MoS

Appendix F – What do we need to disclose – What is Personal Information – a Guide

Appendix G - DSAR: Advanced Searching for Occurrence of Text within eMails

Appendix A:

Schematic thought process to identify who needs to handle any particular requests for information and who is there to help.



Appendix B

Rights of Individuals

THE RIGHT OF ACCESS BY THE DATA SUBJECT (SUBJECT ACCESS REQUEST – UK GDPR Article 15)

What is the right of access?

The right of access, commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data as well as other supplementary information.

[ICO - Right of Access](#)

THE RIGHT TO RECTIFICATION (UK GDPR Article 16 and 19)

The UK GDPR includes a right for individuals to have inaccurate personal data rectified or completed if it is incomplete although this will depend on the purposes for the processing. This may involve providing a supplementary statement to the incomplete data.

This right has close links to the accuracy principle of the UK GDPR (Article 5(1) (d)).

[ICO - Right to Rectification](#)

THE RIGHT TO ERASURE (UK GDPR Article 17 and 19)

Under Article 17 of the UK GDPR individuals have the right to have personal data erased.

This is also known as the 'right to be forgotten'.

The right only applies to data held at the time the request is received. It does not apply to data that may be created in the future. The right is not absolute and only applies in certain circumstances.

[ICO - Right to Erasure](#)

RIGHT TO RESTRICT PROCESSING (UK GDPR Article 18 and 19)

Article 18 of the UK GDPR gives individuals the right to restrict the processing of their personal data in certain circumstances. This means that an individual can limit the way that an organisation uses their data. This is an alternative to requesting the erasure of their data.

[ICO - Right to Restrict Processing](#)

THE RIGHT TO DATA PORTABILITY (UK GDPR Article 20)

Individuals have the right to obtain and reuse their personal data for their own purposes across different services. It allows them to move copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

[ICO - Right to Data Portability](#)

THE RIGHT TO OBJECT (UK GDPR Article 21)

Article 21 of the UK GDPR gives individuals the right to object to the processing of their personal data at any time. This effectively allows individuals to stop or prevent you from processing their personal data.

An objection may be in relation to all of the personal data you hold about an individual or only to certain information. It may also only relate to a particular purpose you are processing the data for.

[ICO - Right to Object](#)

RIGHT NOT TO BE SUBJECT TO AUTOMATED DECISION MAKING AND PROFILING (UK GDPR Article 22)

Article 22 of the UK GDPR has additional rules to protect individuals if you are carrying out solely automated decision-making that has legal or similarly significant effects on them.

[ICO - Rights related to automated decision-making including profiling](#)

Appendix C

Please complete this form in BLOCK CAPITALS

APPLICATION FOR SUBJECT ACCESS TO HEALTH RECORDS

Current data protection legislation, as in
the **Data Protection Act 2018**, the **UK GDPR 2021** and
The Access to Health Records Act 1990

Part A – Identity of the patient about whom the information is being requested:

PATIENT'S DETAILS (records to be accessed)	
Patient's title: (Mr/Mrs/ Miss/Ms/Other)	
Patient's full name:	
Date of Birth:	
Address:	
Postcode:	
Telephone/Contact Number	
NHS and or Hospital Numbers (if known)	

Part B – Details of the information required:

RECORDS REQUIRED	
Details of records required: (Please be as specific as possible e.g., department attended, consultant's name)	
Dates of records required. (e.g., accident date, period of care etc.)	
I wish to (Select <u>one</u>):	View records in person at the hospital
	Have photocopies of the records sent to your address
	Collect photocopies of the records from the hospital
Do you require copies of x-ray reports?	
Do you require medical images on a disc?	

Please be advised that:

1. the overall **Subject Access** process can lawfully take **up to 30 days** (or 1 calendar month) as a minimum, or longer in some circumstances
2. where it is likely to take longer, and that could be **up to 60 or 90 days** for **excessive or complicated** requests, then you will be informed as soon as is reasonably possible
3. **the correct email address** for staff who deal with all patient subject access requests is: dbth.casenoterelease@nhs.net

Part C – Applicant details and declaration:

APPLICANT'S DETAILS (if different from the patient)	
Full name: (including title)	
Address:	
Telephone/Contact number:	
Relationship to patient:	

DECLARATION (please tick one of the following options):	
I am the patient	<input type="checkbox"/>
I have been authorised to act by the patient	<input type="checkbox"/>
I am the patient's parent/legal guardian and have parental responsibility	<input type="checkbox"/>
The patient is over 13 years of age. I am their next of kin/legal representative. I am making this application as they lack the capacity of understanding to make the request themselves and I attach a copy of the authority enabling me to do so e.g., Lasting power of attorney	<input type="checkbox"/>
I have been appointed by the court to manage the patient's affairs and I attach a certified copy of the court order appointing me to do so	<input type="checkbox"/>

IDENTIFICATION REQUIRED (please complete only one option below)

Live Persons	
Please confirm the details of the identification information enclosed with this application. Please refer to the guidance document on what is classed as acceptable forms of ID.	
Please provide the following 2 x proof of identity:	
• Photo ID to confirm your current address	<input type="checkbox"/>
• Non-Photo ID to confirm your current address	<input type="checkbox"/>
Please state which address validation documents you have included:	
Authorisation to act on behalf of a person that lacks capacity (if necessary)	<input type="checkbox"/>

Deceased Persons	
I am the deceased patient's personal representative and attach confirmation of my appointment. For example: (Please tick one of the following options)	
A copy of the will showing the personal representative	<input type="checkbox"/>
Grant of Probate (if a Will is in existence)	<input type="checkbox"/>
Grant of Letters of Administration (if no Will)	<input type="checkbox"/>

I have a claim arising from the individual's death and attach evidence of this. (Please tick one of the following options and explain where necessary)	
A copy of the Will showing the beneficiaries, the evidence of a claim, and/or legal evidence that a Will is being contested	<input type="checkbox"/>
I wish to access information relevant to my claim on the grounds that: (Please provide a lawful reason below):	<input type="checkbox"/>

I declare that the information given is correct to the best of my knowledge and that I am entitled to apply for access to the information detailed above under the terms of the General Data Protection Regulation (GDPR) 2018 or the Access to Health Records Act 1990 (AHRA).

APPLICANT'S SIGNATURE:

.....

DATE:

Part D – Authorisation for application made on behalf of another person:

I hereby request the release of the deceased patient's notes in which I have a legitimate interest and have enclosed proof of my identity and documented evidence to support my request as the deceased's personal representative or to support my claim against the deceased's estate.

Print Name:	Signature:
Date:	

Before returning this form, please ensure that you have:

- a) Signed and dated this form
- b) Completed all relevant sections
- c) Enclosed proof of your identity
- d) Enclosed documentation to support your request (if applying for another person's records)

WARNING - You are advised that the making of false or misleading statements in order to obtain personal information to which you are not entitled is a criminal offence which could lead to prosecution.

Please send the completed form and documentation to:

Casenote Release Department
The Aurora Centre
Doncaster Royal Infirmary
Armthorpe Road,
Doncaster,
DN2 5LT

Tel No: 01302 642235 or 01302 642234

Email: dbth.casenoterelease@nhs.net



**Doncaster and Bassetlaw
Teaching Hospitals**
NHS Foundation Trust

Doncaster Royal Infirmary
Armthorpe Road, Doncaster,
South Yorkshire DN2 5LT

Tel: 01302 366666

Dear Applicant

Thank you for contacting the Trust with regards to the submission of a Subject Access Request (SAR) commensurate with your individual rights under the UK GDPR and the Data Protection Act 2018.

The trust may refuse requests under current legislation where it considers the request to be manifestly unreasonable or excessive. Please would you help us progress your application by focussing your SAR as best you can, and by providing us with any factual evidence that you may have to support your request, should you wish to provide it.

In order to help us resolve your SAR expeditiously, and in any case within 30 to 90 days of the date of your application – permitted under current data protection legislation, especially where there is going to be an excessive amount of work involving numerous staff and information holdings - **we would ask you to complete and return the attached proforma by email to your Divisional General Manager at the email address {insert email}** Please also copy in: dbth.dpo@nhs.net however, it will be your Division, or your Corporate Department who will handle your request, and any questions that you may have should be addressed with them in the first instance.

Alternatively, you may wish to send the completed form to us **by post** to the address below.

Yours sincerely

Divisional GM Name and contact details

Phone number

email address

postal address

Please note that If we do not hear back within 3 months of the date of this letter, then we will consider the matter closed.

APPLICATION FOR SUBJECT ACCESS TO DBTH Paper-based and eRECORDS (Staff)
(under current data protection legislation)

Part A – Identity of the individual member of staff about whom the information is requested:

Please complete this form in BLOCK CAPITALS

APPLICANT'S DETAILS	
Title: (Mr/Mrs/Miss)	
Full name:	
Date of Birth:	
*Address:	
*Postcode	
Personal Telephone number:	
Personal eMail Address:	
DBTH Assignment Number:	

Part B – Details of the information required:

REQUEST DETAILS	
<p>Details of request: Please focus the scope of your request and be as specific as possible e.g. Division/Corporate department/s and where appropriate the names of individual person/s involved etc.</p> <p>If the scope is too broad, excessive, or complex, then we will ask you to focus your request to a more reasonable extent or we may refuse your request. We may also charge a reasonable fee if your request is excessive, although we will always work with applicants to avoid this by using a focussed approach.</p>	
<p>Dates range to be included: Please be as specific as possible</p>	

I declare that the information given is correct to the best of my knowledge and that I am entitled to apply for access to the information detailed above under current data protection legislation.

APPLICANT'S SIGNATURE:

DATE:

Please include copy of your pictorial driving licence or passport in order that we can positively identify you against our DBTH records. Please also note that the address and post code on the identity documents must match the declaration above*.

Internal MoS SAR – Task & Finish Team Notes

Staff Involved

Initials	Name	Department	Contact details where necessary

Sample emails/letter templates are available [here](#).

1.	<p>The SAR request detail:</p> <p>Date received:</p> <p>Target date (30 days: xx/xx/xxxx) <input type="checkbox"/></p> <p>Target date (60 days: xx/xx/xxxx) <input type="checkbox"/> where the applicant has been informed</p> <p>Target date (90 days: xx/xx/xxxx) <input type="checkbox"/> where the applicant has been informed</p> <p>Information requested relates to:</p> <ol style="list-style-type: none"> 1. Internal NHS Mail eMails: YES <input type="checkbox"/> NO <input type="checkbox"/> NB: If YES, then following relevant Appendix A action, the SAR handler should submit their MoS's focussed request to their Divisional/Corporate GM and to copy in the Trust IG Team and the Head of Digital: dbth.dpo@nhs.net 2. Internal Personal/Personnel Documents: YES <input type="checkbox"/> NO <input type="checkbox"/> NB: If YES, then following relevant Appendix A action, the SAR handler should submit their MoS's focussed request to their Divisional/Corporate GM and to copy in the Trust IG Team and the Head of Digital: dbth.dpo@nhs.net 3. Who has looked at my Medical Records: YES <input type="checkbox"/> NO <input type="checkbox"/>
----	--

	<p>NB: If YES, then following relevant Appendix A Taction, the SAR handler should submit their MoS's focussed request to their Divisional GM and to copy in the Trust IG Team and the Head of Digital: dbth.dpo@nhs.net</p> <p>4. Trust phone messages: YES <input type="checkbox"/> NO <input type="checkbox"/> NB: The Trust may only be able to provide telephone messages that have been saved in advance by the recipient.</p> <p>5. WhatsApp Messages: NB: <i>The trust does not support the use of any kind of Social Media messaging platforms, so any applications for same will be refused on those grounds.</i></p> <p>What do they actually want now that you have focussed their application??:</p>
--	---

The Request & any Associated Actions

2.	Actions	Action by/date:
2.1	<p>Send the SAR acknowledgment letter to the applicant as soon as possible after receipt of the application, and where necessary ask for clarification where the request is excessive, or the search scope is too wide.</p> <p>This will generally be covered under the editable version <i>Letter in Appendix D.</i></p>	SAR Response Lead/asap
2.2		

Key SAR etiquette and milestones:

1. Ensure that you agree the scope of the application with the applicant before you start the ICO's 30-day clock ticking
2. Keep the applicant informed
3. Stay within the agreed or informed UK GDPR timescales, or ask for more time

Appendix F

What is personal information: A Guide

What do you need to disclose?

Personal data is information that relates to an identified or identifiable individual.

What identifies an individual could be as simple as a name or a number.

If it is possible to identify an individual directly from the information you are processing, then that information may be personal data.

If you cannot directly identify an individual from that information, then you need to consider whether the individual is still identifiable.

Even if an individual is identified or identifiable, directly or indirectly, from the data you are processing, it is not personal data unless it 'relates to' the individual.

What is the meaning of 'relates to'?

- Information must 'relate to' the identifiable individual to be personal data. This means that it does more than simply identifying them – it must concern the individual in some way.
- To decide whether or not data relates to an individual, you may need to consider:
 - The content of the data – is it directly about the individual or their activities?
 - The purpose you will process the data for; and
 - The results of or effects on the individual from processing the data.
- Data can reference an identifiable individual and not be personal data about that individual, as the information does not relate to them.
- Information that relates to the employee and from which the employee can be identified. In the employment context this would cover, the contract of employment, letters addressed to the employee, medical records, appraisal records, training and development records, disciplinary warnings etc.

What are identifiers and related factors?

- An individual is 'identified' or 'identifiable' if you can distinguish them from other individuals.
- A name is perhaps the most common means of identifying someone. However, whether any potential identifier actually identifies an individual depends on the context.
- A combination of identifiers may be needed to identify an individual.

The UK GDPR provides a non-exhaustive list of identifiers, including:

- Name and surname
- identification (staff) number
- Phone number
- Home address
- Date of Birth

Other factors can identify an individual.

Can we identify an individual directly from the information we have?

- If, by looking solely at the information you are processing you can distinguish an individual from other individuals, that individual will be identified (or identifiable).
- You don't have to know someone's name for them to be directly identifiable, a combination of other identifiers may be sufficient to identify the individual.
- If an individual is directly identifiable from the information, this may constitute personal data.

When can you exclude information?

In the employment context you can exclude information on the following grounds:

1. Information that does not relate to the employee, even if they can be identified from the information. For instance, the HR department may keep a central electronic spreadsheet or table, which tracks sickness absence/lateness/performance/productivity within a particular department. This is unlikely to amount to personal data, even if the employee can be identified, as the focus of the information in the spreadsheet or table relates primarily to the business not the employee. Similarly, Rotas, 'Round Robin' team emails detailing general info and handovers would not be related to the employee.
2. A reference given (or to be given) in confidence for employment, training, or educational purposes. This covers the personal data within the reference whether processed by the reference giver or the recipient.
3. Personal information processed for the purpose of management forecasting or management planning to the extent that complying with the SAR would prejudice the conduct of the business or activity. This gives you considerable flexibility to exclude personal information where an employee is under an internal process. A few HR related examples where you could legitimately exclude are as follows:
 - Workforce restructure: it is likely to prejudice the conduct of a business if information on a workforce restructure programme is disclosed in advance of it being disclosed to the rest of the workforce.
 - Covert investigation: for instance, the accounts department could be looking into fraudulent expense claims in respect of a number of employees, which the employee is unaware of. Disclosing personal information to the employee prior to the conclusion of the covert internal investigation, is likely to prejudice the wider investigation.
 - Complex grievance: a long, drawn-out complex grievance has not yet been concluded, again disclosure of personal information from which the employee can be identified such as witness statements and fact find/interview notes before the grievance is concluded, is likely to prejudice the ongoing grievance investigation.
4. Anything relating to negotiations if disclosure would prejudice the negotiations. So, for instance, discussions have taken place with an employee about leaving the business with an ex-gratia payment. There exists internal communication between HR, Finance and the employee's line manager discussing the terms of the ex-gratia payment and the minimum/maximum that they are prepared to pay. Clearly the

employee can be identified in such communications, but you can legitimately not disclose on the basis that to do so would prejudice the ongoing negotiations.

5. Anything that is legally privileged. Often during an ongoing internal process, you will take legal advice from which the employee can be identified. This can be legitimately excluded when responding to a SAR.

What about information contained in emails?

The contents of emails you store on your computer systems are a form of electronic record to which the general principles above apply. For the avoidance of doubt, you should not regard the contents of an email as deleted merely because a user has moved it to their 'Deleted items' folder.

It may be particularly difficult to find information related to a SAR if it is contained in archived emails that you have removed from your 'live' systems. Nevertheless, the right of access is not limited to personal data that is easy for you to provide. You may, of course, ask the requester to give you some context that would help you find what they want, if you process a large amount of information about them.

It can sometimes be difficult to determine whether an email contains an individual's personal data. This depends on the contents of the email, the context of the information it contains, and what it is being used for. Ultimately it is for you to determine whether any of the information in the email is the individual's personal data. However, you should remember:

The right of access only applies to the individual's personal data contained in the email. This means you may need to disclose *some* or *all* of the email to comply with the SAR.

Just because the contents of the email are about a business matter, this does not mean that it is not the individual's personal data. This depends on the content of the email and whether it relates to the individual.

Just because the individual receives the email, does not mean that the whole content of the email is their personal data. Again, the context of the information and what it is being used for is key to deciding this. However, their name and e-mail address *is* their personal data and you should disclose this information to them.

Example

An employee makes a SAR for all of the information you hold about them. During your search for their personal data, you find 2000 emails which the employee is copied into as a recipient. Other than their name and email address, the content of the emails does not relate to the employee or contain the employee's personal data.

You do not have to provide the employee with a copy of each email (with the personal information of third parties redacted). Since the only personal data which relates to them is

their name and email address, *it is sufficient to advise them that you identified their name and email address on 2000 emails and disclose to them the name contained on those emails, e.g. John Smith, and the email address contained on those emails, e.g. JohnSmith@org.co.uk.* Alternatively, you could provide one email with other details redacted as a sample of the 2000 emails you hold. You should also clearly explain to the individual why this is the only information they are entitled to under the UK GDPR but remember to provide them with supplementary information concerning the processing, e.g., retention periods for the emails.

However, *if any of the content within the email relates to the individual*, you should provide them with a copy of the email itself, redacted if necessary.

What about information we store in different locations?

The right of access applies irrespective of whether the personal data you process is stored in one location or in many different locations. Consolidating disparate data stores may assist you, not just for subject access but in other ways. However, whether this is appropriate for you depends on your circumstances.

What about information stored on personal computer equipment?

You are only obliged to provide personal data in response to a SAR if you are a controller for that data. In most cases, therefore, you do not have to supply personal data if someone else is storing it on their computer systems rather than your own (the exception being where that person is a processor). However, this may not be the case if the requester's personal data is stored on equipment belonging to your staff (such as smartphones or home computers) or in private email accounts or private instant messaging applications.

It is good practice to have a policy restricting the circumstances in which staff may hold information about customers, contacts, or other employees on their own devices, in private email accounts or on private instant messaging applications. Some organisations enable staff to access their systems remotely (e.g. via a secure website), but most are likely to prohibit the holding of personal data on equipment the organisation does not control. Nevertheless, if you do permit staff to hold personal data on their own devices, they may be processing that data on your behalf, in which case it is within scope if you receive a SAR. The purpose for which you hold the information, and its context, is likely to be relevant. We do not expect you to instruct staff to search their private emails, personal devices, or private instant messaging applications in response to a SAR, unless you have a good reason to believe they are holding relevant personal data.

What about other records?

If you hold information about the requester in non-electronic form (e.g., in paper files or on microfiche records), you need to decide whether it is covered by the right of access. You need to make a similar decision if you have removed electronic records from your live systems and archived them in non-electronic form.

Whether the information in hard-copy records is personal data accessible via the right of access depends primarily on whether the non-electronic records are held in a 'filing system'. This is because the UK GDPR does not cover information, which is not, or is not intended to be, part of a 'filing system'.

'Filing system' means any structured set of personal data which is accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

However, under the DPA 2018, personal data held in unstructured manual records processed by public authorities is covered by the right of access. *This includes paper records that are not held as part of a filing system*. Therefore, public authorities may have to search this information to comply with SARs.

Appendix G

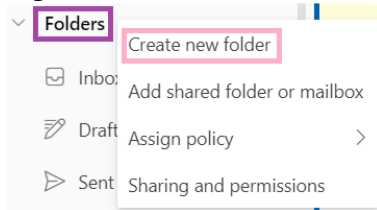
DSAR: Advanced Searching for Occurrence of Text within eMails in Outlook 365 (web) and Post-Search Sifting of Search Results

1. Browse to the NHSmail / 365 portal (<https://portal.nhs.net/>)..



..and click the 'Email' navigation bar option (as indicated by the purple box above) to login and access Outlook 365 Web.

2. Expand (i.e. chevron down) and then right click 'Folders' in the left pane (as indicated by the purple box below) and click 'Create new folder' (as indicated by the pink box below) to make a suitably named folder in your mailbox for the purpose of filing the search outputs – e.g. DSAR-YYYYMMDD to include the current date.

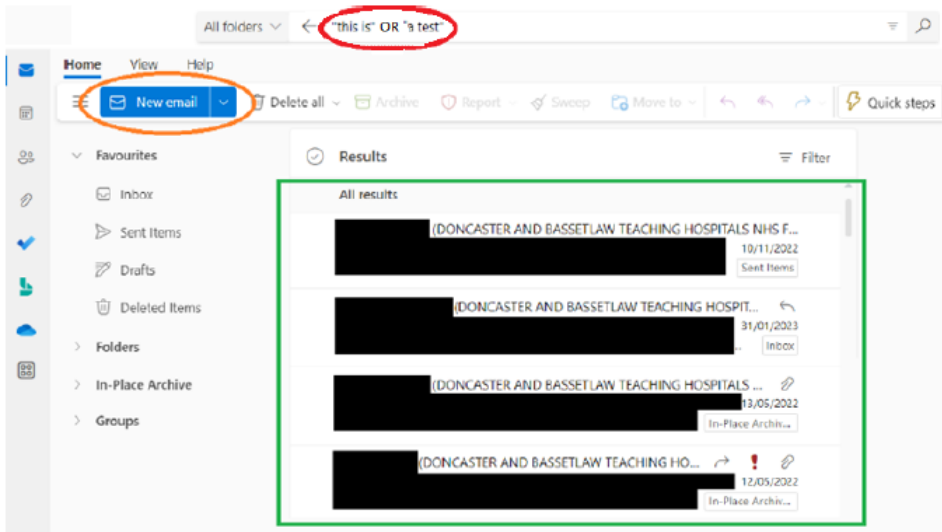


3. In the search box (as indicated by the red ellipse below), enter the terms you are required search for (as per the eMail you have received with this document) and then press the 'Enter' key on your keyboard.

Please note:

You **must** put quotation marks (inverted commas) around each search term **and** include the word 'OR' between each search term, as per the example shown below.

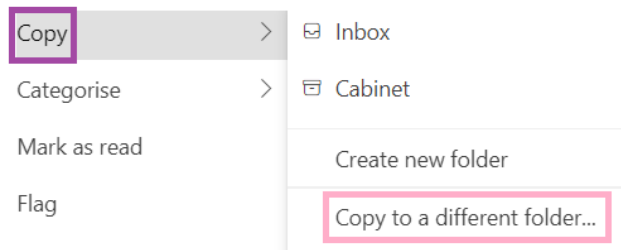
If you have only one search term than there is no need to include the 'OR' statement.



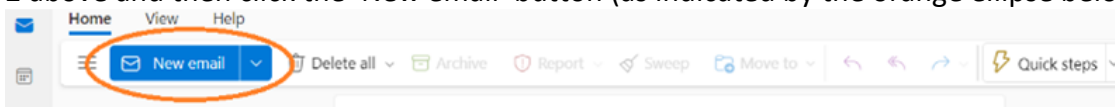
4. Search results will then be displayed as indicated by the green box above, with eMails across all your live NHSmail / 365 mailbox folders and your NHSmail / 365 archive folders filtered in a list, as relevant to the specified search.


5. Click and review each eMail in turn (including attachments) and determine if it is disclosable under the DSAR, referring to the separate guidance provided for that purpose.

If an eMail contains disclosable information, then right click the eMail, click 'Copy' (as indicated by the purple box below), then click 'Copy to a different folder' (as indicated by the pink box below) and select the folder that you created in step 2 above.



6. When step 5 above is completed, in the left pane click the folder that you created in step 2 above and then click the 'New email' button (as indicated by the orange ellipse below).



- Address the eMail to the address indicated by the General Manager
- Enter the eMail subject as: 'DBTH DSAR Return NNN' (where NNN is the number indicated in the eMail you have received with this document)
- Drag and drop each of the matched eMails over to attach into the new eMail
- If the search did not return any matching eMails then enter the text 'Nil found' in the eMail message body
- Click the 'Send' button () to transmit the information

7. If you have previously created or used any Outlook Data Files (also known as “.PST” files) to archive eMails locally then please contact David Linacre (Head of Digital Operations and Cyber Security) for further guidance.

8. Likewise, if you have eMails archived locally from prior to the Trust’s migration to NHSmail (October 2017), and the search request requires inclusion of eMails from that time, then please contact David Linacre (Head of Digital Operations and Cyber Security) for further guidance.

14 – EQUALITY IMPACT ASSESSMENT - PART 1 INITIAL SCREENING

Service/Function/Policy/Project/ Strategy	Division/Executive Directorate and Department	Assessor (s)	New or Existing Service or Policy?	Date of Assessment
IM&T Policy – CORP/ICT 30 v.1	Finance/Digital Transformation & P&OD	Roy Underwood	New	June 2024
1) Who is responsible for this policy? Name of Division/Directorate: Digital Transformation P&OD				
<ul style="list-style-type: none"> Describe the purpose of the service / function / policy / project/ strategy? Who is it intended to benefit? What are the intended outcomes? The scope of this Policy is to ensure that the Trust is compliant with current legislation where there is a one calendar month target to release personal health information from the date of receipt of a valid Subject Access Request (SAR) including a Data Subject Access Request (DSAR) which the Trust labels for any SAR that is requesting personal data that is not of a clinical nature. 				
2) Are there any associated objectives? Legislation, targets national expectation, standards: There are a range of supporting standards defined in Appendix 1 of this policy document.				
3) What factors contribute or detract from achieving intended outcomes? -				
4) Does the policy have an impact in terms of age, race, disability, gender, gender reassignment, sexual orientation, marriage/civil partnership, maternity/pregnancy and religion/belief? Details: [see Equality Impact Assessment Guidance] – None.				
<ul style="list-style-type: none"> If yes, please describe current or planned activities to address the impact [e.g. Monitoring, consultation] - 				
5) Is there any scope for new measures which would promote equality? [any actions to be taken] No.				
6) Are any of the following groups adversely affected by the policy?				
Protected Characteristics		Affected?	Impact	
a) Age		No		
b) Disability		No		
c) Gender		No		
d) Gender Reassignment		No		
e) Marriage/Civil Partnership		No		
f) Maternity/Pregnancy		No		
g) Race		No		
h) Religion/Belief		No		
i) Sexual Orientation		No		
7) Provide the Equality Rating of the service / function /policy / project / strategy – tick (✓) outcome box				
Outcome 1 ✓	Outcome 2	Outcome 3	Outcome 4	
Date for next review: May 2027				
Checked by Rhona McCleery		Date: July 2024		