

Policy Document

Reference: DSP08 (IG08)

Freedom of Information

Version:	10
Date Ratified:	September 2021 by Executive Data Security & Protection Group
To Be Reviewed Before:	July 2023
Policy Author:	Data Security & Protection Manager
Executive Lead:	Senior Information Risk Owner

Version Control Schedule

Version	Issue Date	Comments
1	January 2005	
2	May 2013	Replaces G08 – approved by IGSG to provide definitions of FOI/minor corrections
3	December 2013	Ratified by Quality and Safety Forum. Changes to previous version: <ul style="list-style-type: none"> • Pg. 8 and 9 – remove information re disclosure log • Pg. 11 – information added re-release of band 7 and above info • Pg. 11 – information added re FOI briefing available for staff • Pg. 15 – information added re information in spread sheet format
4	August 2014	<ul style="list-style-type: none"> • Pages 8, 9, 13 – added FOI email address as contact • Page 15 – internal review process updated
5	April 2015	<p>Policy re-written to include more information for Trust staff on processes surrounding FOI</p> <p>Appendix A added to detail Trust process and procedures</p> <p>Appendix B lists exemptions under the FOI Act</p>
6	June 2018	
7	September 2018	
8	January 2019	<ul style="list-style-type: none"> • Page 9 – change of department name and contact details • Page -11-12 additional information regarding disclosure log/public interest test • Appendix A change of time given to respond 8 days from 10 • Page 16 - change of department name and contact details
9	July 2020	<ul style="list-style-type: none"> • Updated to reflect the transfer to IM&T Division • Included justification for seeking applicant ID • Renamed to DSP08
10	September 2021	<p>Minor amends</p> <ul style="list-style-type: none"> • Clarification of timescales for additional/follow-up questions • Page 12 – included a link to the ICO Code of Practice

Statement on Trust Policies

The latest version of 'Statement on Trust Policies' applies to this policy and can be accessed [here](#)

CONTENTS	Page
1. INTRODUCTION	4
2. SCOPE	4
3. DEFINITIONS	4
4. ROLES AND RESPONSIBILITIES	4
5. EDUCATION/TRAINING AND PLAN OF IMPLEMENTATION	8
6. MONITORING AND REVIEW ARRANGEMENTS	8
7. REFERENCES	9
Appendix A: UHNM Freedom of Information Guidance	11
Appendix B: Exemptions provided under the Freedom of Information Act	15
Appendix C: Charges for Information	16

1. INTRODUCTION

The Freedom of Information Act 2000 is part of the Government's commitment to promote openness, transparency and accountability within the public sector. It is a legal requirement that the Trust, along with all other public authorities, must comply with.

The Act applies to all information (excluding personal data which is covered by the Data Protection Act (2018)) held by, or on behalf of the Trust. The Act gives any individual the right to make a written request for information. Compliance of the Act is monitored and enforced by the Information Commissioner's Office (ICO).

The Freedom of Information Act Policy is a statement of the Trust's responsibilities under the legislation and how the Trust ensures compliance with the Act, including procedures staff should follow if they receive a request for information.

An "Equality Impact Assessment" has been completed and no actual or potential discriminatory impact has been identified relating to this document.

2. SCOPE

The procedures within this policy refer to Freedom of Information, but will also be applied to any requests made for environmental information which may be treated under the Environmental Information Regulations (EIR). The minor differences between FOI and EIRs will be taken into account by the FOI Lead when processing the request. This should refer to whom the policy applies and where applicable, the circumstances which apply. The policy applies to all Trust staff and relates to the procedures in place at UHNM.

3. DEFINITIONS

3.1 Personal Identifiable Data (PID)

This describes those items of data concerning a data subject that, if used singly or in conjunction with other data items, could lead to identification of the data subject. Data items include (but are not limited to) name, address, photographs and clinical images, telephone and email contact details.

3.2 Data Protection

An Act of Parliament which defines the UK law on the processing of data of living persons. Data protection defines the principles and is the main legislation governing the protection of personal data in the UK.

3.3 Public Interest Test

Is an assessment carried out by the FOI lead in which the Trust considers the public interest for disclosing and exempting the information which has been requested. The Trust is required to consider the arguments for and against disclosure. The Senior Information Risk Owner must agree the use of a qualified exemption.

4. ROLES AND RESPONSIBILITIES

4.1 Chief Executive

The Chief Executive has the ultimate responsibility for the Trust's compliance with the Act and should ensure that responsibility for reporting FOI issues to the Board is delegated to the appropriate senior level manager.

4.2 Caldicott Guardian

The Trust's Caldicott Guardian has responsibility for patient interests regarding the use of Person Identifiable Data (PID). The Caldicott Guardian is responsible for ensuring records containing PID are stored, accessed and shared in an appropriate and secure manner and particularly that their disclosure is not likely to breach confidentiality laws.

4.3 Senior Information Risk Owner (SIRO)

The Trust SIRO is responsible to the Chief Executive for Data Security & Protection and acts as an advocate for information risk on the Trust Board.

4.4 Data, Security and Protection Officer (Corporate Records)

The Head of Data Security & Protection/Data Protection Officer has overall responsibility for the provision of the FOI service and the FOI Officer operationally ensures Trust procedures and processes are in place to comply with the Act. The FOI Officer can be contacted via foi@UHNM.nhs.uk the key responsibilities are to:

- ensure that the Trust complies with all aspects of the Act, associated Codes of Practice and related provisions;
- provide reports to the Board (or equivalent) highlighting resource, performance and compliance issues;
- draft and / or maintain the currency of the Trusts FOI policy;
- ensure that all staff are aware of their personal responsibilities for compliance with the Act and adhere to Trust policies and procedures;
- ensure training and written procedures are widely disseminated and available to all staff;
- ensure the general public has access to information about their rights under the Act;
- establish appropriate arrangements to deal with appeals and investigations into complaints about decisions and response times;

4.5 Data Security & Protection Operational Group (DSPOG)

The DSPOG receives regular FOI performance reports which highlight:

- numbers of FOI requests received;
- numbers responded to within the 20 working day limit;
- exemptions applied;
- details of any complaints made about any response or the process itself;
- details of any requests that have been escalated to the Information Commissioner's Office by the applicant.

Based on these reports the DSPOG agree any necessary improvement plans and recommendations for improvements, for example identify additional resources if there is continued failure to meet statutory deadlines, increasing staff awareness through additional training or guidance materials

4.6 Data Security & Protection Executive Group (DSPEG)

The DSPEG receives regular reports and updates on the compliance status of the FOI service. This Group receives assurance that the Trust is meeting its statutory obligations and provides that assurance to the Trust Board, via the Performance and Finance Committee.

4.7 Senior Management

All corporate information should be created with the awareness that a request for this information may be received and information which is not exempt must be disclosed to comply with the Act. Senior members of staff should therefore, ensure that they (and their staff) receive training via Trust Induction, statutory & mandatory training alongside information on the DSP Intranet site to ensure they are able to adhere to policies, procedures and guidance.

4.8 All Staff

All staff should be made aware of their own personal responsibilities for the creation of records including emails which may be subject to disclosure under the Freedom of Information Act. In addition, each member of staff should be aware of the organisation's process for dealing with a FOI request which is received by them, for example who to contact and the urgency for doing so due to the strict time limits which the law applies.

All staff should be aware that information regarding AfC Band 7 and above staff will be released if requested. This applies to corporate/Trust information (i.e., work contact details) not personal information. AfC bands and job descriptions will be released for all Trust roles if requested.

RECEIVING AND RESPONDING TO FOI REQUESTS WITHIN THE TRUST

Appendix A sets out the Trust's procedures for responding to requests made under the FOI Act. All Trust employees should be aware of these procedures.

The Trust will ensure it meets the duty of a public authority to provide advice and assistance to persons who propose to make (or who have already made) requests for information under the Act. This is as set out in section 16 of the Act.

The Trust has a duty to "confirm or deny" whether information requested is held. Unless an exemption applies, the Trust must confirm or deny whether information is held.

The Trust may not have to comply with a request if an exemption applies. Exemptions allowed for under the Act are specific – a list can be found in appendix B. The Trust is obliged to disclose any information requested unless an exemption can be shown to apply. If an exemption applies, the requestor shall be informed of this within the usual 20 working day limit. Any follow-up questions/queries as the result of an FOI disclosure will attract an additional 20 working day limit, in accordance with ICO guidance.

Section 14 of the Act allows for a request to be exempt by categorising it as "vexatious" or "repeated". The Trust will review the history of the request to establish whether the section 14 exemption can be applied. Vexatious requests may be obsessive and cause unjustified distress/disruption. A requestor themselves cannot be made vexatious – it is the requests themselves that are assessed, not the individual person; future request from the same person will not be automatically refused, they will be assessed to see if they can be complied with or not. Decisions to use the section 14 exemption should be agreed by the Data Security & Protection Manager and the Head of Data Security & Protection/ Data Protection Officer (IM&T Division).

Requestors deemed as vexatious or repeated must be given the right to appeal this decision. Once a requestor has been informed that their request is deemed vexatious the Trust is not obliged to provide any further response to repeated requests or requests for substantially similar information until a reasonable interval of time has passed.

A number of organisations use the FOI legislation to conduct a campaign, for example medical directories requesting information on drug usage. Pseudonyms are used to avoid meeting the threshold of a Section 12 exemption. In these circumstances, where a campaign is suspected, the Trust is within its rights to seek confirmation of ID (ICO Guidance - Recognising a request made under the Freedom of Information Act (section 8) Version 1.2). It should be noted that in these circumstances, the Trust is not refusing to provide the information and will aggregate requests, working with the applicant to provide as much assistance as possible.

The Trust can refuse to process a request for information if the costs associated with that request would exceed £450. This equates to 18 hours work at the flat rate of £25 per hour. This is regardless of salary or job role. Not all activities associated with the production of information will be chargeable. This is in line with section 12 of the Act. When the section 12 exemption is intended to be used, a breakdown of the work involved in completing the request will be required by the Data Security & Protection (DSP)

department, showing how the £450 limit would be exceeded. The applicant may wish to pay for the request to be completed. A charging schedule is provided in appendix C.

The Trust will follow the appeals procedure in point 9 of appendix A when dealing with complaints regarding FOI requests.

If a request is received for information that is subject to a current piece of work, the Trust may deem its premature disclosure to not be in the public interest and the Trust may therefore temporarily withhold the release of such information.

If an applicant wishes to use information provided by the Trust for commercial purposes, written permission must be gained from the Trust under the Regulation on the Re-use of Public Sector Information Regulations (2005). This may involve a licensing arrangement, which may incur a fee for the applicant.

RELEASE OF TRUST EMPLOYEE NAME AND DETAILS

The Trust is a public authority and there is recognised justification for the disclosure of employee names and contact details.

It is Trust policy that the names and contact details of Consultants, medical staff, and other staff members whose names/details already appear on the Trust's public website will be released without gaining further consent.

The Trust will routinely release names and contact details of executive directors, associate directors, clinical directors, clinical leads, directorate managers, matrons, and other staff at band seven or above.

For other staff, consent will usually be asked for if release of names is appropriate. There may be occasions where the public interest in disclosing personal details may be judged to outweigh an individual's preference to restrict such disclosure. The final decision of release of information remains with the persons responsible for FOI compliance within the Trust.

Staff with public facing roles are more likely to have their information released. Personal contact details such as home address, home telephone number, and personal email address will never be released in response to an FOI request.

Requests for salary information will be answered by providing Agenda for Change (AfC) pay bands. Where a salary falls outside of the AfC bands their salary will be given in £10,000 bands. Executive director salaries are available via the Trust annual report.

CONSULTATION WITH THIRD PARTIES

It is acknowledged that disclosure of some information held by the Trust would affect the legal rights of a third party. Unless an exemption from the Act applies in relation to the requested information the Trust is obliged to disclose the information requested.

The Trust will try to liaise with third parties where appropriate to gain their opinion on disclosure. Failure for the third party to respond does not relieve the Trust of its duties under the Act. The Trust must still reply to the requestor within the twenty working day timeframe.

In every case, it is the Trust, and not the third party (or their representative) to determine whether the information is disclosed or not. Refusal from the third party for information to be disclosed does not mean information will ultimately be withheld.

When entering into contracts the Trust will refuse to include contractual terms which aim to restrict the disclosure of information held by the Trust or the contract itself.

RECORDS MANAGEMENT

A request for information cannot be refused because a department/the Trust is unable to locate a document or information due to poor records management.

It is a criminal offence to destroy material because it has been requested under the FOI Act.

The Trust's Records Management & Information Lifecycle Policy contains information about the creation and management of Trust records.

Information in spread sheets will be saved in a "csv" format before being sent to the requestor. Pivot tables will not be released due to their ability to store "hidden" identifiable data.

Spread sheets may be made publically available via the publication scheme as necessary in line with the Government's transparency agenda. The Trust's Publication Scheme can be found within the Privacy Notice, which is [here](#).

DISCLOSURE LOG

In addition to proactively updating its Publication Scheme, the Trust will develop and maintain an online disclosure log that identifies the main types of requests received and the responses given.

A disclosure log lists responses to requests made to us under the FOI Act which are felt to be of wider public interest.

The Trust will assess each response to determine if it should be published in the disclosure log and will make a judgement accordingly by typically using the following criteria:

Demonstrable evidence that key decisions have been made within the Trust:

- If disclosure passes the Public Interest Test;
- Where UHNM has spent public money or disclosed information around resources.

The Trust will not publish any requests from a complainant for correspondence on their complaint file.

5. EDUCATION/TRAINING AND PLAN OF IMPLEMENTATION

An overview of this document is provided to staff via the Data Security & Protection (DSP) e-learning or face to face training sessions. If changes are made to this document the DSP training is updated and staff notified via mass communication.

Bespoke training regarding FOI is available to all staff and can be arranged via the Freedom of Information Lead.

6. MONITORING AND REVIEW ARRANGEMENTS

6.1 Monitoring Arrangements

The Corporate Records Working Group (which is an operation sub-group feeding into the DSPOG) will monitor the operational implementation of this Policy, and any subsequent revisions, as part of the Annual Data Security & Protection toolkit return. This is carried out by collecting evidence that the correct actions have been completed.

FOI activity reports will be made regularly to the DSPOG, including the numbers of FOI Requests received, answered, within time limit together with a cumulative summary of performance against target (95% compliance). These reports will provide evidence of compliance with the legislation.

Highlight reports will be presented to the Data Security & Protection Executive Group to provide assurance that the Trust is meeting its obligations. This information will be presented to the Trust Board via the Performance and Finance Committee.

6.2 Review

This Policy is subject to review when any of the following conditions are met:

- The adoption of the Policy highlights errors or omissions in its content;
- Where other policies/strategies/guidance issued by the Trust conflict with the information contained herein;
- Where the procedural or guidance framework of the NHS evolves/changes such that revision would bring about improvement;
- 3 year elapses after approval of the current version.

7. REFERENCES

Human Rights Act 2000

This Act became law on 2 October 2000. It binds public authorities including Health Authorities, Trusts, Primary Care Groups and individual doctors treating NHS patients to respect and protect an individual's human rights. This will include an individual's right to privacy (under Article 8) and a service user's right to expect confidentiality of their information at all times.

Article 8 of the Act provides that 'everyone has the right to respect for his private and family life, his home and his correspondence'. However, this article also states 'there shall be no interference by a public authority with the exercise of this right except as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention or disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others'.

Each organisation must act in a way consistent with these requirements. It must take an individual's rights into account when sharing personal information about them.

Freedom of Information Act 2000

This Act came into force in November 2000 and will be fully in force during the coming years. The Information Commissioner (previously the Data Protection Commissioner) will oversee the implementation of this Act. This Act gives individuals rights of access to information held by public authorities – this becomes effective in 2005. Further information will be available as implementation progresses (see www.dataprotection.gov.uk).

Access to Health Records Act 1990

This Act gives patient's representatives right of access to their manually held health records, in respect of information recorded on or after 1 November 1991. This Act is only applicable for access to deceased person's records. All other requests for access to information by living individuals are provided under the access provisions of the Data Protection Act 2018.

Data Protection Act 2018/General Data Protection Regulation

The Data Protection Act 2018 is the vehicle which allows the UK to enact the provisions of the General Data Protection Regulations (the EU-wide standard for the maintenance of data subjects' privacy). It allows data subjects extensive rights in relation to their personal data and reinforces the security and protection requirements of that data.

Health & Social Care Act 2001: Section 60

Section 60 of the Health and Social Care Act 2001 makes it lawful to disclose and use confidential patient information in specified circumstances where it is not currently practicable to satisfy the common law confidentiality obligations. This is intended primarily as a temporary measure until anonymisation measures or appropriate recording of consent can be put in place. Where the powers provided by this legislation are used to support the processing of confidential patient information there will be additional safeguards and restrictions on the use and disclosure of the information. These may differ from case to case and change over time where the process of annual review, required by the legislation, results in more stringent safeguards being applied.

UHNH Freedom of Information Guidance

1. Purpose

This document provides practical guidance on how to deal with requests for information to ensure the Trust complies with the Freedom of Information Act.

2. Background

- 2.1 The Freedom of Information Act gives individuals the right to make a written request for access to information held by the Trust. If the information is held by the Trust it must be disclosed in accordance with the Act.
- 2.2 Requests are 'applicant blind', meaning the Trust is unable to take the identity of the applicant into consideration to determine if information should be released or withheld.
- 2.3 Requests are 'purpose blind' meaning the Trust is not permitted to enquire why the information has been requested.
- 2.4 Applications for information under the Act may not always be successful. The Trust may no longer hold the information which has been requested or it may be withheld if an exemption can be applied – see Appendix B.

3. What to do if you receive a written request

- 3.1 FOI is governed by strict timescales. Requests should be sent via the internal mail or email to the FOI team within 24 hours of receipt (FOI@uhnm.nhs.uk)
- 3.2 The 20 day statutory response time starts from the day the request is received by the Trust, not when it reaches the Freedom of Information Lead.

4. What to do when the DSP Officer (Corporate Records) asks you for information

- 4.1 Any member of staff may be approached to provide information in part or in full in order for the Trust to respond to a FOI and is expected to make every effort to respond to the team by the date given. If staff are unable to provide, or are unsure, they should contact the FOI lead immediately.
- 4.2 If the information is readily available it should be returned immediately in order that the Trust can meet the statutory deadlines. If the same information is requested on numerous occasions then consideration must be given to including it in the publication scheme.
- 4.3 If staff believe that they are unable to provide the information within 8 days then the FOI lead should be informed at the earliest opportunity.
- 4.4 If staff have not responded to a request for information within 10 days the matter will be escalated to the Data Security & Protection Manager who will liaise with the appropriate director.
- 4.5 Under section 16 of the Freedom of Information Act, the Trust has a duty to provide advice and assistance to applicants and the Trust will make every effort to meet this. If you cannot provide the information requested, but could suggest an alternative, then contact the FOI lead at the earliest opportunity.

5. Transferring a request

- 5.1 A request can only be transferred outside of the Trust if the **DSP Officer (Corporate Records)** has received written consent from the requester that it is ok to do so.
- 5.2 A request can only be transferred outside of the Trust if the information being requested is not held, but is held by another public authority. If the Trust holds some of the information requested, a transfer can only be made in respect to the information not held. The Trust will advise the requester that it does not hold part, or all, of the information requested.
- 5.3 Under Section 45 of the Freedom of Information Act If the Trust believes that some or all of the information requested is held by another public authority we can suggest the applicant applies directly to them. The response should include the contact details of the public authority, or consult another authority to confirm that it holds the information and (with the applicants written consent) transfer the request.

6. What the DSP Officer (Corporate Records) does with a request

- 6.1 A request will be logged and acknowledged within 48 hours of receipt by the FOI lead.
- 6.2 The request will be checked and if the information is available on the Trust's Publication Scheme the link will be sent to the applicant.
- 6.3 If the information requested is not on the Publication Scheme, and the information is not held by the FOI lead, a request will be sent to the nominated manager for the department to provide the information.
- 6.4 If the information is not exempt from disclosure, it will be collated by the FOI team and a final response will be drafted for approval by the Data Security & Protection Manager, Head of Communications and the relevant Executive Director.
- 6.5 If the information is exempt from disclosure, the applicant will be informed (in writing) which exemption applies. They will be given the right to appeal the decision and details of this will be given with the response. A list of exemptions is at Appendix B.
- 6.6 Where the use of a qualified exemption is proposed, a Public Interest Test will need to be carried out and approval of the qualified exemption will be sought from the Information Governance Manager and Senior Information Risk Owner and obtaining approval via the Executive Director of Strategy and Business Development and the Company Secretary.

7. Vexatious/Repeated Requests

- 7.1 The **DSP Officer (Corporate Records)** has overall sight of all requests coming into the Trust and will identify any requests which fall within the definition of Vexatious or Repeated (according to the FOI Legislation and the ICO Code of Practice ([What if we want to refuse a request as vexatious or repeated?](#))).
- 7.2 Where a request is deemed to fall within this category, the **DSP Officer (Corporate Records)** will apply Section 14 of the legislation and seek approval from the Data Security & Protection Manager and the Head of Data Security & Protection, the decision to be ratified by the Trust Caldicott Guardian before responding to the applicant.

8. Access to Health Records

- 8.1 If the applicant is requesting a copy of their own health records they will be informed that their request is exempt under section 40(1) of the Freedom of Information Act and will be advised how to make a Subject Access Request.

8.2 The Data Protection Act applies to requests for access to Health Records and other Personal Identifiable Data. If staff are unsure about personal identifiable information then please contact the Data Security & Protection Manager.

9. Environmental Information Regulations

9.1 Requests for information regarding environmental elements (air, water, land etc.) noise, activities which effect the environment and some aspects of health and safety are treated under the Environmental Information Regulations (EIR).

9.2 Requests for information under EIR should be processed in the same way as FOI, and passed to the FOI lead, the only difference being they can be requested verbally.

10. Requests for review

10.1 If a requester would like to appeal they should be advised to put this in writing and submit to FOI@UHNM.nhs.uk

10.2 On receipt of a request for review the **DSP Officer (Corporate Records)** or Data Security & Protection Manager should prepare a timeline of the Trust's handling of the FOI and liaise with the The Head of Data Security & Protection/ Data Protection Officer (IM&T Division) to ask them to conduct an independent review. The Head of Data Security & Protection/ Data Protection Officer (IM&T Division) may liaise with other staff as necessary. The Head of Data Security & Protection/ Data Protection Officer (IM&T Division) is not involved with initial FOI responses and is therefore an independent reviewer. The Corporate Governance Department will then be informed and asked for opinions from a relevant Executive Director. DSPEG are informed of requests for reviews.

10.3 If, after the requester has appealed the Trust's decision and they are still not satisfied they may appeal to the Information Commissioner's Office at the address below:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

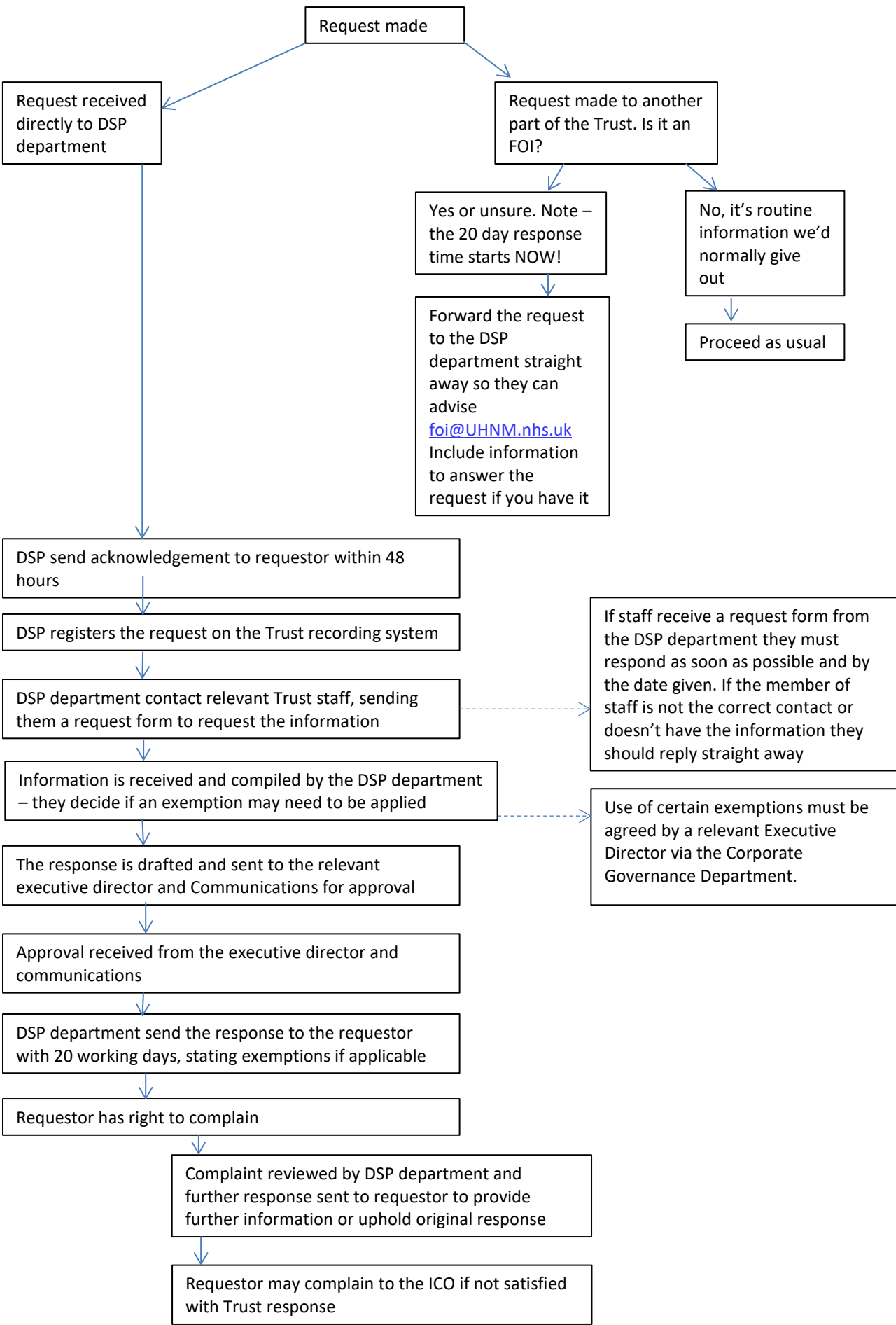
11. Charges and Fees

11.1 Information in the Trust's Publication Scheme is available to view and download free of charge.

11.2 Charges may be levied for hard copies, multiple copies, or copying onto other forms of media. Charges will be in accordance to the Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004.

11.3 See Appendix C of this policy for further information regarding charging.

University Hospitals of North Midlands NHS Trust
 DSP08 (IG08) Freedom of Information



Exemptions provided under the Freedom of Information Act

Absolute - no public interest test required

Qualified - public interest test* is required

Section	Exemption	Absolute or Qualified
12	Cost of compliance is excessive	No public interest test is required but you must provide an estimate of cost to the FOI lead
14 (1)	Vexatious request	No public interest test required
14(2)	Repeated request	No public interest test required
21	Information reasonably accessible to the applicant by other means	Absolute
22	Information intended for future publication	Qualified
23	Information supplied by or relating to security bodies	Absolute
24	National security	Qualified
26	Defence	Qualified
27	International relations	Subject to Prejudice Test
28	Relations within the UK	Qualified
29	Economy	Qualified
30	Investigations	Qualified
31	Law enforcement	Qualified
32	Information contained in court records	Absolute
33	Public audit	Qualified
34	Parliamentary privilege	Absolute
35	Policy formulation, Ministerial communications, Law Officers advice and operation of Ministerial Private Office	Qualified
36	Effective conduct of public affairs	Qualified
37	Communications with Her Majesty and the awarding of honours	Qualified
38	Health & Safety	Qualified
39	Environmental Information	Treat under EIR
40	Personal information	Absolute
41	Information provided in confidence	Consider public interest under Common Law
41	Information provided in confidence relating to contracts	Absolute
42	Legal professional privilege	Qualified
43	Commercial interest – Public sector contracts. Commercial detriment of third parties	Qualified
44	Prohibitions on disclosure	Absolute

* - qualified exemptions must be approved by a relevant Executive Director, via the Corporate Governance Department. They will look at the weight of arguments for releasing or not releasing the information in line with the exemption guidance provided by the Act and the ICO.

Charges for Information

In line with the Freedom of Information Act, reasonable charges can be made for excessive and/or additional copies of information. The following charging scheme will be used by the Trust:

Photocopying/Printing	
A4 black and white	5 pence per side
A3 black and white	10 pence per side
Postage	Standard 2 nd class mail charges (unless otherwise requested)

Charges will not be made unless the cost of providing the information totals more than £20.

As outlined by the Freedom of Information Act, charges for information cannot be made unless this totals over £450. This is calculated by staff time being charged at £25 per hour therefore the maximum time limit is 18 hours. Any request which the cost of compliance is estimated over £450 will be exempt under section 12 of the Act.