Wirral Community Health and Care NHS Foundation Trust

Freedom of Information Policy
IG09
Version 6

TRUST-WIDE NON-CLINICAL

Document detail	
Policy Number	IG09
Version	Version 6
Approved by	Finance and Performance Committee
Effective from	08/2022
Date of last review	04/2025
Date of next review	04/2028
Lead Director	Senior Information Risk Owner
Responsible Lead	Information Governance Lead / Data Protection Officer
Superseded documents	Freedom of Information Policy and Procedures
Document summary	Freedom of Information Act 2000, Environmental Information Regulation 2004, public authorities, information requests, 20 working days, exemptions

Document History		
Version number	Comments	Approved by
4	Review of Policy	Quality and Safety Committee
5.1	Oversight moved from Quality & Safety Committee to the Finance and Performance Committee	Finance and Performance Committee August 2024
6	Updated in line with lifecycle	Finance and Performance Committee April 2025

Policy on a page

The Freedom of Information (FOI) Act 2000 places a number of obligations on public authorities to provide access to disclosable records. The FOI Act does not give people access to their own personal data (information about themselves); this is a right under Data Protection Legislation. See the Individual Rights and Accessing Records Policy.

Anyone can make an FOI request. The request must be in writing, include the requester's real name, include an address for correspondence and describes the information requested. The Trust has 20 working days to respond to a request.

Requests should be made in writing to wcnt.foi@nhs.net or to Information Governance, Wing 5 First Floor, St Catherine's Health Centre, Derby Road, Birkenhead, CH42 0LQ.

Once the Information Governance / Record Keeping Officer has recorded the request on the Excel FOI management document, the request will be sent by the Information Governance / Record Keeping Officer to an identified FOI response lead (based on the subject of the request) along with the date the internal response is due. The agreed internal response time is 10 working days.

The Act only covers recorded information the Trust holds. The Trust doesn't have to make up an answer or find out information from elsewhere if the relevant information isn't already in recorded form.

The Trust must not make any changes or deletions as a result of the request - this is a criminal offence.

The Trust can refuse an entire request under the following circumstances:

- *It would cost too much / take too much staff time to deal with the request*
- *The request is vexatious*
- *The request repeats a previous request from the same person*

In addition, the FOI Act contains a number of exemptions that allow the Trust to withhold information from a requester.

The Information Governance / Record Keeping Officer or Information Governance Lead /Data Protection Officer should be provided with all requested information by the FOI response lead. They will then review the information and advise the Trust's SIRO if they believe that the Trust should refuse to comply with a request or apply an exemption. Based on the specialist advise provided, the SIRO will make the final decision on refusals and application of exemptions.

All final FOI response letters will be reviewed and signed off by the Trust's SIRO. In the SIRO's absence responses will be reviewed and signed off by the most appropriate Director in relation to the nature of the request.

The Information Governance Lead / DPO will complete any requested internal review. The Chief Executive Officer will review all internal reviews prior to the release.

The ICO has a general duty to investigate complaints from members of the public who believe that an authority has failed to respond correctly to a request for information.

SUPPORTING STATEMENTS

This document should be read in conjunction with the following statements:

SAFEGUARDING IS EVERYBODY'S BUSINESS

All Wirral Community Health and Care NHS Foundation Trust employees have a statutory duty to safeguard and promote the welfare of children and adults, including:

- being alert to the possibility of child/adult abuse and neglect through their observation of abuse, or by professional judgement made as a result of information gathered about the child/adult;
- knowing how to deal with a disclosure or allegation of child/adult abuse;
- undertaking training as appropriate for their role and keeping themselves updated;
- being aware of and following the local policies and procedures they need to follow if they have a child/adult concern';
- ensuring appropriate advice and support is accessed either from managers, *Safeguarding Ambassadors* or the Trust's safeguarding team;
- participating in multi-agency working to safeguard the child or adult (if appropriate to your role; ensuring contemporaneous records are kept at all times and record keeping is in strict adherence to Wirral Community Health and Care NHS Foundation Trust policy and procedures and professional guidelines. Roles, responsibilities and accountabilities, will differ depending on the post you hold within the organisation;
- ensuring that all staff and their managers discuss and record any safeguarding issues that arise at each supervision session.

EQUALITY AND HUMAN RIGHTS

Wirral Community Health and Care NHS Foundation Trust recognises that some sections of society experience prejudice and discrimination. The Equality Act 2010 specifically recognises the protected characteristics of age, disability, gender, race, religion or belief, sexual orientation and transgender. The Equality Act also requires regard to socio-economic factors including pregnancy/maternity and marriage/civil partnership.

The Trust is committed to equality of opportunity and anti-discriminatory practice both in the provision of services and in our role as a major employer. The Trust believes that all people have the right to be treated with dignity and respect and is committed to the elimination of unfair and unlawful discriminatory practices.

Wirral Community Health and Care NHS Foundation Trust also is aware of its legal duties under the Human Rights Act 1998. Section 6 of the Human Rights Act requires all public authorities to uphold and promote Human Rights in everything they do. It is unlawful for a public authority to perform any act which contravenes the Human Rights Act.

Wirral Community Health and Care NHS Foundation Trust is committed to carrying out its functions and service delivery in line with a Human Rights based approach and the FREDA principles of **F**airness, **R**espect, **E**quality **D**ignity and **A**utonomy.

CONTENTS **Page No.**

1. PURPOSE AND RATIONALE

The Freedom of Information (FOI) Act 2000 places a number of obligations on public authorities to provide access to disclosable records. Consequently, the FOI Act applies to Wirral Community Health and Care NHS Foundation Trust (WCHC).

The FOI Act does not give people access to their own personal data (information about themselves) such as their health records or credit reference file. If a member of the public wants to see information that a public authority holds about them, they would need to submit an access request under UK Data Protection legislation.

In general members of the public have a statutory right to request information held by a public authority regardless of when it was created, by whom or the form in which it is now recorded.

To support compliance with FOI Act the Trust;

- offers a single point of access for requests via wcnt.foi@nhs.net or Information Governance, Quality and Governance, Wing 5 First Floor, St Catherine's Health Centre, Wirral, Birkenhead, CH42 0LQ
- provides a detailed publication scheme on its website
- works in partnership with other trusts and stakeholders as appropriate to manage and respond to requests
- trains staff to recognise FOI requests

The purpose of this policy is to inform staff of the processes in place to ensure Trust compliance with the FOI Act 2000.

2. OUTCOME FOCUSED AIMS AND OBJECTIVES

This policy was produced in order to achieve Trust compliance with the FOI Act.

Staff should refer to and follow the process outlined in this policy if they receive an FOI request and if they are identified as internal FOI lead for the requested information.

3. SCOPE

This Policy applies to all employees of Wirral Community Health and Care NHS Foundation Trust, this includes bank staff, individuals on secondment and trainees or those on a training placement within the Trust as well as locum or temporary staff employed through an agency.

4. DEFINITIONS (Glossary of Terms)

Glossary of Terms	Definition
Exemptions	There are nine categories of exemptions under the FOI Act. If a document meets the criteria for one of these categories, a public authority can refuse to release it.
Vexatious	Disproportionate or unjustifiable level of distress, disruption or irritation

5. RESPONSIBILITIES, ACCOUNTABILITIES AND DUTIES

Chief Executive Officer
The Chief Executive Officer has overall accountability and responsibility for Trust compliance with the FOI Act. The Chief Executive Officer will review internal review responses prior to release (see section 6 of this policy).

Trust Board
The Board will review FOI concerns escalated from the Information Governance and Data Security Group via the Quality & Safety Committee and Finance & Performance Committee.

Finance and Performance Committee
The Finance and Performance Committee (FPC) is the responsible committee for reviewing, approving and monitoring adherence with the Freedom of Information Policy.
Freedom of Information figures are reported to the Finance and Performance Committee (FPC) via the Information Governance and Data Security Group. The FPC will review concerns escalated to them, action those relevant to the Committee's terms of reference and refer, as appropriate, to the Board.

Senior Information Risk Owner
The Trust's Senior Information Risk Owner (SIRO) has executive responsibility for the management and mitigation of all information risk.

SIRO will:

- review FOIs received by the Information Governance / Record Keeping Officer or Information Governance Lead / DPO
- liaise with the Information Governance / Record Keeping Officer or Information Governance Lead / DPO regarding complex FOI request
- make the final decision on refusals and application of exemptions

Information Governance and Data Security Group
The Trust's Information Governance and Data Security Group is responsible for reviewing and approving this policy prior to ratification by FPC.

The Information Governance and Data Security Group will review and monitor number of FOIs received, themes of FOIs and compliance with regulatory time scales.

Information Governance Lead **/Data Protection Officer**
The Information Governance Lead is the author of this policy and is responsible for overseeing the day-to-day management of FOI requests. The Information Governance Lead /Data Protection Officer will:

- ensure compliance with the FOI Act
- maintain the policy and publication scheme to promote FOI awareness
- escalate any delays in response by internal services to the SIRO
- review and advise on complex FOI responses collated by the Information Governance / Record Keeping Officer prior to submission to the SIRO

Information Governance / Record Keeping Officer
The Information Governance / Record Keeping Officer is responsible for the day-to-day management and coordination of FOI requests. The Information Governance / Record Keeping Officer will:

- receive and coordinate all FOI requests and responses
- escalate any delays in response by the internal services to the Information Governance Manager / Data Protection Officer
- formulate FOI response letters
- request FOI response review of complex requests by the Information Governance Manager / Data Protection Officer prior to submission to the SIRO
- report FOI compliance to the monthly Information Governance and Data Security Group

Heads of Service/Locality Leads/FOI Leads
Managers at all levels are responsible for ensuring that staff that they manage are aware of and adhere to this policy. Managers of services must ensure that they and their staff respond fully and promptly to requests for information by the Information Governance / Record Keeping Officer or Information Governance Lead / Data Protection Officer. Any issues relating to time frame compliance by FOI Leads should be escalated to the Information Governance / Record Keeping Officer or the Information Governance Manager.

Joint Union Staff Side (JUSS)
JUSS representatives have an important part to play in providing advice, support and if required, representation to their members as well as working in partnership with managers and the HR team to ensure the Freedom of Information policy is applied fairly and consistently across the Trust.

All Staff
All staff are responsible for adhering to this policy. Staff are responsible for ensuring that they identify and report FOI requests to the Information Governance / Record Keeping Officer or Information Governance Lead / Data Protection Officer promptly.

6. PROCESS

The FOI Act 2000 provides public access to information held by public authorities. It does this in two ways:

- public authorities are obliged to publish certain information about their activities; and
- members of the public are entitled to request information from public authorities.

The Act covers any recorded information that is held by a public authority in England, Wales and Northern Ireland, and by UK-wide public authorities based in Scotland. Information held by Scottish public authorities is covered by Scotland's own Freedom of Information (Scotland) Act 2002.

Public authorities include government departments, local authorities, the NHS, state schools and police forces.

Recorded information includes, printed documents, computer files, letters, emails, photographs, and sound or video recordings.

Publication Scheme

The Information Commissioners Office (ICO) produced guidance on the kinds of information health bodies in England should provide in order to meet their requirements under the model publication scheme:

- Who we are and what we do - organisational information, structures, locations and contacts
- What we spend and how we spend it- financial information relating to projected and actual income and expenditure, procurement, contracts and financial audit
- What our priorities are and how we are doing – strategies and plans, performance indicators, audits, inspections and reviews
- How we make decisions – decision making processes and records of decisions
- Our policies and procedures – current written protocols, policies and procedures for delivering services and responsibilities
- Lists and register
- The services we offer – information about the services we offer, including leaflets, guidance and newsletters

The Trust will publish the information above and FOI response letters on Wirral Community Health and Care NHS Foundation Trust's website. The Information Governance / Record Keeping Officer will share FOI response letters redacted of personal data with the Trust's Communications Team monthly.

Who can make a request?

Anyone can make an FOI request – they do not have to be UK citizens, or resident in the UK. FOI requests can also be made by organisations, for example a newspaper, a campaign group, or a company. Employees of a public authority can make requests to their own employer, although good internal communications and staff relations will normally avoid the need for this.

What makes a request valid?

To be valid under the Act, the request must:

- be in writing. This could be a letter or email. Requests can also be made via the web, or even on social networking sites such as Facebook or Twitter
- include the requester's real name.
- include an address for correspondence. This need not be the person's residential or work address – it can be any address at which you can write to them, including a postal address or email address.
- describe the information requested. Any genuine attempt to describe the information will be enough to trigger the Act, even if the description is unclear, or too broad or unreasonable in some way. The Act covers information not documents, so a requester does not have to ask for a specific document.

Even if a request is not valid under the FOI Act it does not necessarily mean it can be ignored. Requests for 'environmental information' under the Environmental Information Regulation 2004, for example, can be made verbally. The Trust is also obliged to provide advice and assistance to requesters. Where somebody seems to be requesting information but has failed to make a valid freedom of information request, the Trust should draw their attention to their rights under the Act and tell them how to make a valid request.

Making a request

Requests should be made in writing to wcnt.foi@nhs.net or to Information Governance, Wing 5 First Floor, St Catherine's Health Centre, Derby Road, Birkenhead, CH42 0LQ. If services receive a written FOI they must share the FOI with the Information Governance team immediately.

Once a request is received

When an application for information is received the following information will be recorded by the Trust onto the Excel FOI management document:

- Initial date received by the Trust
- Name of applicant
- Email address / address of requester
- Access route
- Information requested
- FOI response lead
- Date that internal response is due
- Date that external response is due

How long does the Trust have to comply with a request?

The obligation under the Act is to respond to requests promptly, with a time limit acting as the longest time the Trust can take. Under the Act, most public authorities may take up to **20 working days** to respond, counting the first working day after the request is received as the first day.

The time allowed for complying with a request starts when the Trust receives it, not when it reaches the Information Governance / Record Keeping Officer or Information Governance Lead / Data Protection Officer. All requests that are either identified as an FOI request or are being treated as one in the case where the nature of the request is unclear must be forwarded to the Information Governance / Record Keeping Officer or Information Governance Manager / Data Protection Officer immediately. The FOI team can be contacted at wcnt.FOI@nhs.net

Certain circumstances may allow for extra time to respond. However, in all cases the requester must be provided with a written response within the standard time limit for compliance.

Once the Information Governance / Record Keeping Officer has recorded the request on the Excel FOI management document the request will be sent by the Information Governance / Record Keeping Officer to the FOI response lead along with the date the internal response is due. The agreed internal response time is 10 working days.

What if the Trust is unsure what's being asked for?

Requests are often ambiguous, with many potential interpretations, or no clear meaning at all. In these instances, the allocated FOI response lead should contact the Information Governance / Record Keeping Officer and ask them to contact the requester as soon as possible for clarification. The Trust does not have to deal with the request until clarification is received. However, the Trust must consider whether the requester requires advice and assistance to enable them to clarify or rephrase their request. For example, the Trust may explain what options are available to them and ask whether any of these would adequately answer their request.

What if the Trust doesn't have the information?

The Act only covers recorded information the Trust holds. When compiling a response to a request for information, the Trust may have to draw from multiple sources of information, but the Trust doesn't have to make up an answer or find out information from elsewhere if the relevant information isn't already in recorded form.

The Trust must carry out adequate and directed searches for information prior to concluding

that no recorded information is held. If a requester complains to the ICO that the Trust haven't identified all the information held, the ICO will consider the scope, quality and thoroughness of the searches and test the strength of reasoning and conclusions.

If the Trust does not hold the requested information the FOI response lead must notify the Information Governance / Record Keeping Officer. The Information Governance / Record Keeping Officer will produce a letter that advises the requester that the Trust does not hold the requested information and request SIRO sign off.

Do we have to tell the requester what information the Trust holds?

Yes, unless one of the reasons for refusing applies – see **'When can the Trust refuse a request?'**

The Trust has two duties when responding to requests for information:

- to let the requester know whether the Trust holds the information
- to provide the information

In some circumstances, the Trust can refuse to confirm or deny whether the information is held. For example, if a requester asks about evidence of criminal activity by a named individual, saying whether the Trust holds such information could be unfair to the individual and could prejudice any police investigation. This is called a 'neither confirm nor deny' (NCND) response.

Can the Trust change or delete requested information?

No, normally the Trust should disclose the information held at the time of the request. The Trust are however allowed to make routine changes to the information while dealing with the request as long as these would have been made regardless of the request.

The Trust must not make any changes or deletions as a result of the request, for example, because the information could be seen as embarrassing if it was released. This is a criminal offence.

In what format should the information be provided?

There are a number of ways the Trust could make information available, including by email, as a printed copy, on a disk, or by arranging for the requester to view the information. Normally, the information will be sent by whatever means is most reasonable. For example, if the requester has made their request by email, and the information is an electronic document in a standard form, then the Trust would reply by email and attach the information.

However, requesters have the right to specify their preferred means of communication, in their initial request.

The Information Governance / Record Keeping Officer or Information Governance Lead / Data Protection Officer will oversee all communication with the requester.

When can the Trust refuse a request?

A requester may ask for any information that is held by a public authority. However, this does not mean the Trust are always obliged to provide the information. In some cases, there will be a good reason why the Trust should not make public some or all of the information requested.

The Trust can refuse an entire request under the following circumstances:

- It would cost too much or take too much staff time to deal with the request
- The request is vexatious
- The request repeats a previous request from the same person

Further information regarding the specifics of refusing entire requests on the grounds of the circumstances listed is available on the ICO website.

In addition, the FOI Act contains a number of exemptions (see below) that allow the Trust to withhold information from a requester. In some cases, it will allow the Trust to refuse to confirm or deny whether you hold information.

Some exemptions relate to a particular type of information, for instance, information relating to government policy. Other exemptions are based on the harm that would arise or would be likely arise from disclosure, for example, if disclosure would be likely to prejudice a criminal investigation or prejudice someone's commercial interests.

There is also an exemption for personal data if releasing it would be contrary to UK General Data Protection Regulation (UK GDPR) or the Data Protection Act 2018 (DPA 2018).

The Trust can automatically withhold information because an exemption applies only if the exemption is 'absolute'. This may be, for example, information received from the security services, which is covered by an absolute exemption. However, most exemptions are not absolute but require application of a public interest test. This means the Trust must consider the public interest arguments before deciding whether to disclose the information. Consequently, the Trust may have to disclose information in spite of an exemption, where it is in the public interest to do so.

The Information Governance / Record Keeping Officer or Information Governance Lead /Data Protection Officer will advise the Trust's SIRO if they believe that the Trust should refuse to comply with a request or apply an exemption. The SIRO will make the final decision on refusal and application of exemptions.

What exemptions are there?

Some exemptions apply only to a particular category or class of information, such as information held for criminal investigations or relating to correspondence with the royal family. These are called class-based exemptions.

Some exemptions require you to judge whether disclosure may cause a specific type of harm, for instance, endangering health and safety, prejudicing law enforcement, or prejudicing someone's commercial interests. These are called prejudice-based exemptions.

The Act also often refers to other legislation or common law principles, such as confidentiality, legal professional privilege, or data protection. In many cases, the Trust may need to apply some kind of legal 'test' - it is not as straightforward as identifying that information fits a specific description. It is important to read the full wording of any exemption, and if necessary consult ICO guidance, before trying to rely on it.

How does the Trust decide whether disclosing information would cause prejudice?

For the purpose of the Act, 'prejudice' means causing harm in some way. Many of the exemptions listed below apply if disclosing the information held would harm the interests covered by the exemption. In the same way, confirming or denying whether the Trust have the information can also cause prejudice. Deciding whether disclosure would cause prejudice is called the prejudice test. To decide whether disclosure (or confirmation/denial) would cause

prejudice, the Trust:

- must be able to identify a negative consequence of the disclosure (or confirmation/denial), and this negative consequence must be significant (more than trivial);
- must be able to show a link between the disclosure (or confirmation/denial) and the negative consequences, showing how one would cause the other; and
- there must be at least a real possibility of the negative consequences happening

Detailed guidance on the Prejudice Test can be found on the ICO's website.

All FOI exemptions can be found in Part II of the FOI Act, at sections 21 to 44. Below is a list of exemptions available:

Section 21 – information already reasonably accessible
Section 22 – information intended for future publications
Section 22a – research information
Sections 23-24 – security bodies and national security
Sections 26-29 – requests that would prejudice defence, effective armed forces, international relations, relations between the UK government, the Scottish Executive, the Welsh Assembly and the Northern Ireland Executive, economy or the financial interests of the UK, Scottish, Welsh or Northern Irish administrations
Sections 30 and 31 – investigations and prejudice to law enforcement
Section 32 – court records
Section 33 – prejudice to audit functions
Section 34 – parliamentary privilege
Sections 35 and 36 – government policy and prejudice to the effective conduct of public affairs
Section 37 – communications with the royal family and the granting of honours
Section 38 – endangering health and safety
Section 39 – environmental information
Section 40(1) – personal information of the requester
Section 40(2) – data protection
Section 41 – confidentiality
Section 42 – legal professional privilege
Section 43 – trade secrets and prejudice to commercial interests
Section 33 – prohibitions on disclosure

The Information Governance / Record Keeping Officer or Information Governance Lead /Data Protection Officer should be provided with all requested information by the FOI response lead. They will review the information and advise the Trust's SIRO if they believe that the Trust should refuse to comply with a request or apply an exemption. The SIRO will make the final decision on refusals and application of exemptions.

Final responses to FOI requests

All final FOI response letters will be reviewed and signed off by the Trust's SIRO. In the SIRO's absence responses will be reviewed and signed off by the most appropriate Director in relation to the nature of the request.

The Freedom of Information Act and Data Protection

UK GDPR and the DPA 2018 provide rules for handling information about people. They include the right for people to access their personal data. FOI Act 2000 and UK GDPR/DPA 2018 come under the heading of information rights and are regulated by the ICO.

When an individual requests access to their own information, they are applying their right to access under UK data protection legislation. Right to access is commonly referred to as a Subject Access Request. However, members of the public often wrongly think it is the Freedom of Information Act that gives them the right to access their personal information. For further information on the rights of data subjects please see the Individual Rights and Accessing Records Policy.

UK GDPR and the DPA 2018 exist to protect people's right to privacy, whereas the Freedom of Information Act is about ridding unnecessary secrecy. These two aims are not necessarily incompatible but there can be a tension between them and applying them sometimes requires careful judgement.

Consequently, when someone makes a request for information that includes someone else's personal data, the Trust will need to carefully balance the case for transparency and openness under the FOI Act against the data subject's right to privacy under UK data protection legislation. The Information Governance / Record Keeping Officer or Information Governance Lead will need to decide whether information can be released without infringing the UK GDPR data protection principles.

Internal Reviews

How should we handle a complaint?

Any disputes or complaints arising from the outcome or handling of a request for information will be recorded on the Trust's reporting system, Datix. The Datix report will include the outcome of any internal review, along with timescales. Under the FOI Act this procedure is known as an internal review and demonstrates a commitment to openness and transparency.

The Trust includes a paragraph in all response letters issued that informs requesters how to request an internal review and their right to complain to the ICO under Section 50 of the FOI Act should they be unhappy following the review outcome.

What constitutes a request for an internal review?

If the Trust receives a complaint which seeks to challenge the outcome of the initial response, then the Trust will treat this as a request for an internal review. An internal review request must be made in writing to the Trust, in line with requests for information under FOI Act.

What are the timescales for an internal review?

Internal review requests should be made within 40 working days of the initial response. This deadline is communicated in the Trust's response letter. The Trust are not obliged to provide a review if it is requested after 40 working days.

The Information Governance / Record Keeping Officer will acknowledge an internal review request and provide a target date for response, which should usually be within 20 working days.

There may be circumstances where the Trust require more time to complete an internal review. In these circumstances the Information Governance / Record Keeping Officer will inform the requestor that you will need more time and provide a reasonable target date. This will be no more than an additional 20 working days, unless there are legitimate reasons why a longer extension is necessary.

As with requests for information, if the Trust require clarification for an internal review request,

then the timescale to respond does not start until the clarification is provided.

How should we conduct an internal review?

The Information Governance Manager / Data Protection Officer will complete Trust internal reviews unless they were actively involved in the initial response. Internal reviews will be reviewed and signed off by the Chief Executive Officer.

Internal reviews should consider how the request was handled and the initial response, whether the relevant information was identified, and whether you wish to uphold the original exemptions or whether the Trust wish to apply a different or additional exemption(s).

If the Trust decide to provide the requestor with information which was withheld previously then the Trust will supply it at the same time as the internal review outcome, or at least notify the requestor of when it will be provided.

The Trust will inform the requester of their right to appeal to the ICO.

ICO Complaints

The ICO has a general duty to investigate complaints from members of the public who believe that an authority has failed to respond correctly to a request for information. If someone makes a complaint against the Trust, the ICO complaints handling process gives the Trust an opportunity to reconsider actions and put right any mistakes without us taking any formal action. If the complaint is not resolved informally, the ICO will issue a decision notice. If the ICO identify that the Act has been breached, the decision notice will say what the Trust need to do to put things right.

The Trust would be breaching the FOI Act if we:

- fail to respond adequately to a request for information.
- fail to adopt the model publication scheme, or do not publish the correct information; or
- deliberately destroy, hide or alter requested information to prevent it being released

The last point is the only criminal offence in the Act that individuals and public authorities can be charged with.

7 CONSULTATION

This policy has been reviewed by the Information Governance and Data Security Group prior to submission to the FPC.

8. TRAINING AND SUPPORT

Staff are required to complete the Trust's information governance training annually (e-Learning for Healthcare Data Security Awareness Level 1) through ESR.

Information governance training is mandatory for all staff that have access to Trust information.

Managers with management responsibility for staff will be responsible for monitoring staff compliance with e-Learning for healthcare Data Security Awareness Level 1 and for ensuring that staff have sufficient time to complete training.

Bespoke information governance training will be provided by the Information Governance Lead on request by managers that have identified a training need within their team.

Staff with specialist roles are required to complete additional data security and protection training suitable to their role. Additional training requirements will be identified through the annual Training Needs Analysis.

Compliance with mandatory annual information governance training and training for staff with specialist roles will be monitored by the Information Governance and Data Security Group.

9. MONITORING

The effectiveness of this policy will be assessed by the Information Governance and Data Security Group. The Information Governance / Record Keeping Officer reports total number of FOIs received each month, those responded to within timescale, rationale for any delayed responses and will inform the group of any internal reviews.

The Information Governance and Data Security Group Action Log and Minutes are shared with both QSC and FPC for monitoring and assurance purposes.

The Information Governance Lead / Data Protection Officer will monitor the Trusts Publication Scheme to ensure adherence to guidance set out by the ICO.

See Appendix B.

10. EQUALITY AND HUMAN RIGHTS ANALYSIS

An Equality Impact Assessment has been completed and can be found in Appendix A.

11. LINKS TO OTHER POLICIES

Individual Rights and Accessing Records Policy
Information Governance Policy
Confidentiality and Data Protection Policy
Records Management Policy

Appendix A: Equality Impact Assessment

Title	Freedom of Information Policy
What is being considered?	This policy was produced in order to achieve compliance with the FOI Act. Staff should refer to this policy when they receive FOI requests and follow the instructions provided within this policy.
Who may be affected?	Patients [x] Staff [x] Public [x] Partner agencies [x]

Is there potential for an adverse impact against the protected groups below? Age, Disability, Gender Reassignment, Marriage and Civil Partnership, Pregnancy and Maternity, Race, Religion and Belief, Sex (gender), Sexual Orientation or the Human Rights articles?	Yes [ ] No [x]

On what basis was this decision made? (Please complete for both 'yes' and 'no').
Anyone can make an FOI request.
Under the FOI Act any one can make an FOI request. If a requester has a disability or requires translation / interpretation support the Governance Officer / Information Governance Manager / Data Protection Officer will coordinate access to such support and adjust the request process to ensure accessibility for all.

Discussion held with Equality Manager.

With regard to the general duty of the Equality Act 2010, the above function is deemed to have no equality relevance.

Equality relevance decision by Karen Clearkin Title / Committee Risk and Governance Manager

Date 28 March 2025

Appendix B: Monitoring Compliance with the process described in the policy

Minimum requirement to be monitored	Process for monitoring (e.g. audit)	Responsible individual / group/ committee	Frequency of monitoring	Evidence	Responsible individual for development of action plan	Responsible committee for monitoring of action plan and Implementation
Number of FOIs, % responded to in time frame, rationale for delay and themes	Data recorded by IG Team and reported at Information Governance and Data Security Group	Information Governance / Record Keeping Office Information Governance Lead /DPO Information Governance and Data Security Group	Monthly	Information Governance and Data Security Group Minutes and Action Log	Information Governance Lead / DPO	Finance and Performance Committee
Compliance with publication scheme guidance set out by ICO	Ensuring FOIs are sent on a monthly basis to the Communications team so anonymised FOIs can be added to the Trust's public website	Information Governance / Record Keeping Office Information Governance Lead /DPO	Monthly	Published FOIs on Trust public facing website	Information Governance Lead / DPO	Finance and Performance Committee