FOI REF: 26/599

29th September 2026

East Sussex Healthcare NHS Trust

Eastbourne District General Hospital
Kings Drive
Eastbourne
East Sussex
BN21 2UD

Tel: 0300 131 4500
Website: www.esht.nhs.uk

Further to your recent request for information made under the Freedom of Information Act (FOIA) 2000, I now set out our answers to your specific questions, and any clarifications sought and provided, as follows:

I am writing to request the following recorded information under the Freedom of Information Act 2000. Please treat this as a request under both the FOIA 2000 and the Environmental Information Regulations 2004, as applicable to each part. The request relates to your organisation's handling of Freedom of Information (FOI) and Environmental Information Regulations (EIR) requests.

1. **The name of any case management or software system currently used to log, track and manage FOI/EIR requests, including any modules, add-ons or configured tools (for example a CRM, case management platform, shared mailbox or SharePoint list) used for this purpose.**

   Under Section 31(1)(a) of the Freedom of Information Act (FOIA), the Trust can confirm that it holds information relevant to your request, however, we are unable to disclose it for the reasons explained below.

   Historically, we would disclose information relevant to the Trust's IT systems, infrastructure and software as part of our transparency agenda under the terms of the Freedom of Information Act (FOIA). However, in light of the recent cyber-attacks on NHS hospitals and the serious impact these have had on patient services and the loss of patient data, we are having to reconsider this approach. Please see several links to news articles about these recent cyber incidents provided below for your information.

   - *NHS England — London » Synnovis Ransomware Cyber-Attack*
   - *NHS England confirm patient data stolen in cyber attack - BBC News*
   - *Merseyside: Three more hospitals hit by cyber attack - BBC News*

   As a result of these attacks, thousands of hospital and GP appointments were disrupted, operations were cancelled, and confidential patient data was stolen which included patient names, dates of birth, NHS numbers and descriptions of blood tests.

   When we respond to a Freedom of Information request, we are unable to establish the intent behind the request. Disclosure under the FOIA involves the release of information to the world at large, free from any duty of confidence. Providing information about our

systems or security measures to one person is the same as publishing it for everyone. While most people are honest and have no intention of misusing information to cause damage, there are criminals who look for opportunities to exploit system weaknesses for financial gain or to cause disruption.

In the context of the FOIA, the term ‘’public interest’’ does not refer to the private or commercial interests of a requestor; its meaning is for the “public good”. The Trust receives a significant number of requests each year regarding our IT systems, infrastructure and cyber security measures. Most of these requests are commercially driven and serve no direct public interest. Information relevant to our IT portfolio is often requested by consultancy companies who then pass on this information to their client base. Many of these requests are submitted through the FOI portal whatdotheyknow.com who publish our responses, making this information available to an even wider audience.

As a large NHS Trust we hold extensive personal data relevant to our patients and staff, much of which is considered very sensitive. A lot of this information is held electronically on various administration and clinical systems. We have a duty under the Data Protection Act 2018 and the UK GDPR to protect this personal information and take all necessary steps to ensure this data is kept safe. This means not disclosing information that could allow criminals to gain unlawful access to our systems and infrastructure. The Trust can be heavily fined should it be found to have acted in a negligent way which results in a personal data breach. We need to demonstrate that we comply with our legal obligations under data protection and freedom of information legislation, but we must be careful that too much transparency does not result in harm to our patients or staff, or cause disruption to our services.

Moreover, under the Network and Information Systems (NIS) Regulations Act 2018, operators of essential services such as NHS organisations like ours have a legal obligation to protect the security of our networks and information systems in order to safeguard our essential services. By releasing information that could increase the likelihood or severity of a cyber-attack, the Trust would fail to meet its security duties as stated in Section 10 of the Network and Information Systems Regulations 2018. Should we not comply with these requirements regulatory action can be taken against the Trust. Further information about the Network and Information Systems (NIS) Regulations Act 2018 can be found here – The Network and Information Systems Regulations 2018: guide for the health sector in England - GOV.UK.

Your request asks for specific details regarding our IT Systems which, for the reasons explained above, would be inappropriate to release into the public domain. If disclosed, it is possible that patient data as well as other confidential information would be put at risk. Such disclosure could also impact on the security of our systems and result in serious disruption to the health services we deliver to the local community. Section 31(1)(a) of FOIA provides that information is exempt if its disclosure would, or would be likely to, prejudice (a) the prevention or detection of crime. In this case, disclosure would be likely to prejudice the prevention of crime by enabling or encouraging malicious acts which could compromise the Trust’s IT systems and infrastructure. The Trust’s capacity to defend itself from such acts relates to the purposes of crime prevention and therefore Section 31(a) exemption is applicable in these circumstances. For these reasons, the Trust considers disclosure of the information you are seeking to be exempt under Section 31(1)(a) [law enforcement] of the FOIA and the information requested is being withheld in its entirety and the names of IT Systems within the attached extract from the

FOI policy. The full wording of Section 31 can be found here: Freedom of Information Act 2000.

Section 31 is a qualified exemption and therefore we must consider the prejudice or harm that may be caused by disclosure of the information you have requested, as well as apply a public interest test that weighs up the factors in maintaining the exemption against those in favour of disclosure.

In considering the prejudice or harm that disclosure may cause, as explained should the Trust release information into the public domain which draws attention to any weaknesses relevant to the security of our systems or those of a supplier, this information could be exploited by individuals with criminal intent. Increasing the likelihood of criminal activity in this way would be irresponsible and could encourage malicious acts which could compromise our IT systems or infrastructure, result in the loss of personal data and/or impact on the delivery of our patient services. We consider these concerns particularly relevant and valid considering the increasing number of cyber incidents affecting NHS systems in recent years and the view by government, the ICO and NHS leaders that the threat of cyber incidents to the public sector is real and increasing.

- *Organisations must do more to combat the growing threat of cyber attacks | ICO*

In the Government's Cyber Security Strategy 2022-2030, the Chancellor of the Duchy of Lancaster and Minister for the Cabinet Office states on page 7:

"Government organisations - and the functions and services they deliver - are the cornerstone of our society. It is their significance, however, that makes them an attractive target for an ever-expanding army of adversaries, often with the kind of powerful cyber capabilities which, not so long ago, would have been the sole preserve of nation states. Whether in the pursuit of government data for strategic advantage or in seeking the disruption of public services for financial or political gain, the threat faced by government is very real and present.

Government organisations are routinely and relentlessly targeted: of the 777 incidents managed by the National Cyber Security Centre between September 2020 and August 2021, around 40% were aimed at the public sector. This upward trend shows no signs of abating."

With this in mind, we then considered the public interest test for and against disclosure. It should be noted that the public interest in this context refers to the public good, not what is 'of interest' to the public or the private or commercial interests of the requester. In this case we consider the public interest factors in favour of disclosure are:

- Evidences the Trust's transparency and accountability
- Provides information relevant to the IT systems and applications the Trust uses
- Reassures the public and partners that the Trust procures these systems in line with Procurement legislation
- Reassures the public and partners that the Trust's IT infrastructure and systems are secure

Factors in favour of withholding this information are:

- Public interest in crime prevention
- Public interest in avoiding disruption to our health services
- Public interest in maintaining the integrity and security of the Trust's systems
- Public interest in the Trust avoiding the costs associated with any malicious acts (e.g. recovery, revenue, regulatory fines)
- Public interest in complying with our legal obligations to safeguard the sensitive confidential information we hold

In considering all of these factors, we have concluded that the balance of public interest lies in upholding the exemption and not releasing the information requested. Although disclosure would provide transparency about our software systems and IT infrastructure, this is outweighed by the harm that could be caused by people who wish to use this information to assess any vulnerabilities in our security measures and consequently use this information for unlawful purposes. Cybercrime can not only lead to major service disruption but can also result in significant financial losses. As a publicly funded organisation, we have a duty for ensuring our public funding is protected and spent responsibly. Moreover, as a public body the Trust must demonstrate that it keeps its confidential data and IT infrastructure safe and complies with relevant legislation, but at the same time we must be vigilant that transparency does not provide an opportunity for individuals to act against the Trust. In considering the impact that recent cyber-attacks have had on NHS services, including the cancellation of thousands of patient appointments and procedures as well as the loss of confidential patient data, we consider the overriding public interest lies in withholding this information. The private or commercial interests of a requester should not outweigh the public interest in protecting the integrity of our systems and continuity of our essential patient services. Although we appreciate there may be legitimate intentions behind requesting this information, we must take a cautious approach to requests of this nature and appreciate your understanding in this matter.

It is important to note that the Trust and its commissioning partners are required to follow very specific rules when procuring equipment or services. Information about procurement and tendering can be found on our website –

Governing documents, incorporating: Standing Orders, Standing Financial Instructions, Scheme of Delegation.

To contact the Procurement Service, please email - esht.procurement@nhs.net.

2. **A copy or extract of any recorded documentation (for example internal guidance, process maps or handling procedures) describing how FOI/EIR requests are logged, tracked and managed. If no such documentation is held, please confirm that.**

Please see the attached document for an extract, Sections 6.1 to 6.4, of the FOI policy.

Please note that the FOI policy, including the process for logging, tracking and managing FOI's, is being updated to reflect improvements to service provision.

Please also note we are applying Section 31(1)(a), as we have redacted the name of the Trust's IT System from the attached document, please refer to question 1.

3. **The number of full-time equivalent (FTE) staff involved in processing FOI/EIR requests, and the job titles of those roles. I am not requesting the names of any individuals; job titles or role descriptions are sufficient.**

The Freedom of Information (FOI) Team at East Sussex Healthcare NHS Trust (ESHT) consists of 2.0 WTE as follows:

Role	Number of Staff	Total WTE
Senior FOI Administrator	1	0.8
Corporate Governance Assistant	2	1.2

4. **Any recorded information describing how FOI/EIR requests are assigned and coordinated across the organisation — for example, whether a central team handles requests end-to-end, or whether requests are passed to individual departments or teams to respond directly. If no such information is held, please confirm that.**

We do not hold any other FOI handling procedural documentation to that disclosed in our response to Question 2.

5. **Any recorded information setting out internal target response times for FOI/EIR requests in addition to the statutory 20 working day deadline — for example internal service level agreements, process checklists or workflow timelines. If no such information is held, please confirm that.**

We do not hold any other FOI handling procedural documentation to that disclosed in our response to Question 2.

6. **For each of the last five financial years ending 31 March (2021-22, 2022-23, 2023-24, 2024-25 and 2025-26), please provide separately for each year:**

6.1 The number of FOI requests received

6.2 The number of EIR requests received

ESHT records EIR requests in the same way as FOI's requests, so we cannot provide a breakdown between the two. The data requested is as follows:

Metric	2021/22	2022/23	2023/24	2024/25	2025/26
EIR/FOI Requests Received	699	798	939	909	920

6.3 The number of Subject Access Requests (SARs) received

The SARs data is as follows:

Metric	2021/22	2022/23	2023/24	2024/25	2025/26
SAR's Received	2,640	3,096	3,272	4,014	3,998

6.4 The number of each of the above completed within the applicable statutory timeframe

The following table reflects the number of EIR/FOI requests and SAR's closed in each year that were closed within their respective timeframes:

Metric	2021/22	2022/23	2023/24	2024/25	2025/26
EIR/FOI Requests Closed In Time	554	653	714	796	761
SAR's Closed In Time	N/A*	N/A*	3,255	3,306	3,860

*Please note that this data was not captured due to a change in the software used to manage SAR's

I trust this information is helpful in its detail or explanation however, if you are dissatisfied with the response, then you have the right to request an internal review. If you wish to seek an internal review, please write to the Freedom of Information Team at esh-tr.foi@nhs.net quoting the above FOI reference number, within 40 working days. Please note the Trust is not obliged to accept a request for an internal review after this time period.

Yours faithfully

Freedom of Information (FOI) Team
East Sussex Healthcare NHS Trust
0300 131 4716
Core Hours of Business: Monday to Friday 9.00am to 4.00pm

6.1 Using the Process

This process should always be followed when responding to requests for information under the Act. Where appropriate, responses to requests for environmental information will use the same procedures as for responding to FOI requests, whilst recognising that there are some differing regulations between EIR and FOI on the provision of information. These include rules governing what environmental information may be disclosed (exceptions under EIR) and the requirement to respond to requests for environmental information whether the request is in writing or verbal form. Subject Access Requests should be referred immediately to the Request for Information Department (e-mail: esh-tr.SAR@nhs.net) to be handled in accordance with the Data Protection Act.

As information is made available by the Trust to stakeholders through staff on a daily basis, these procedures will not apply in all circumstances. Use of the procedures will not be required where:

- The information is already reasonably accessible to the applicant by other means, e.g., publicity leaflets and other reference material.
- Information is released as part of the Trust's normal business process, e.g., job application packs, information provided to a service user about their treatment or care.
- The correspondence is not a request for information.
- The request does not include a name and/or correspondence address.
- The request is not made in writing (an e-mail will be classed as a written request) - not applicable to environmental information requests.
- It is a request for access to health records or other personal data under the Data Protection Act.

6.2 Dealing with Initial Application for Information (see figure 1)

All staff have a responsibility to deal with any request they may receive. Many applicants may not make their requests for information directly to the Freedom of Information team. Support will be provided to enable people with a disability to put their requests in writing.

Please note that the process for dealing with an EIR request is the same as for an FOI request, but that EIR requests can be received verbally.

Figure 1 details the process that all staff should follow when an initial application for information is made.

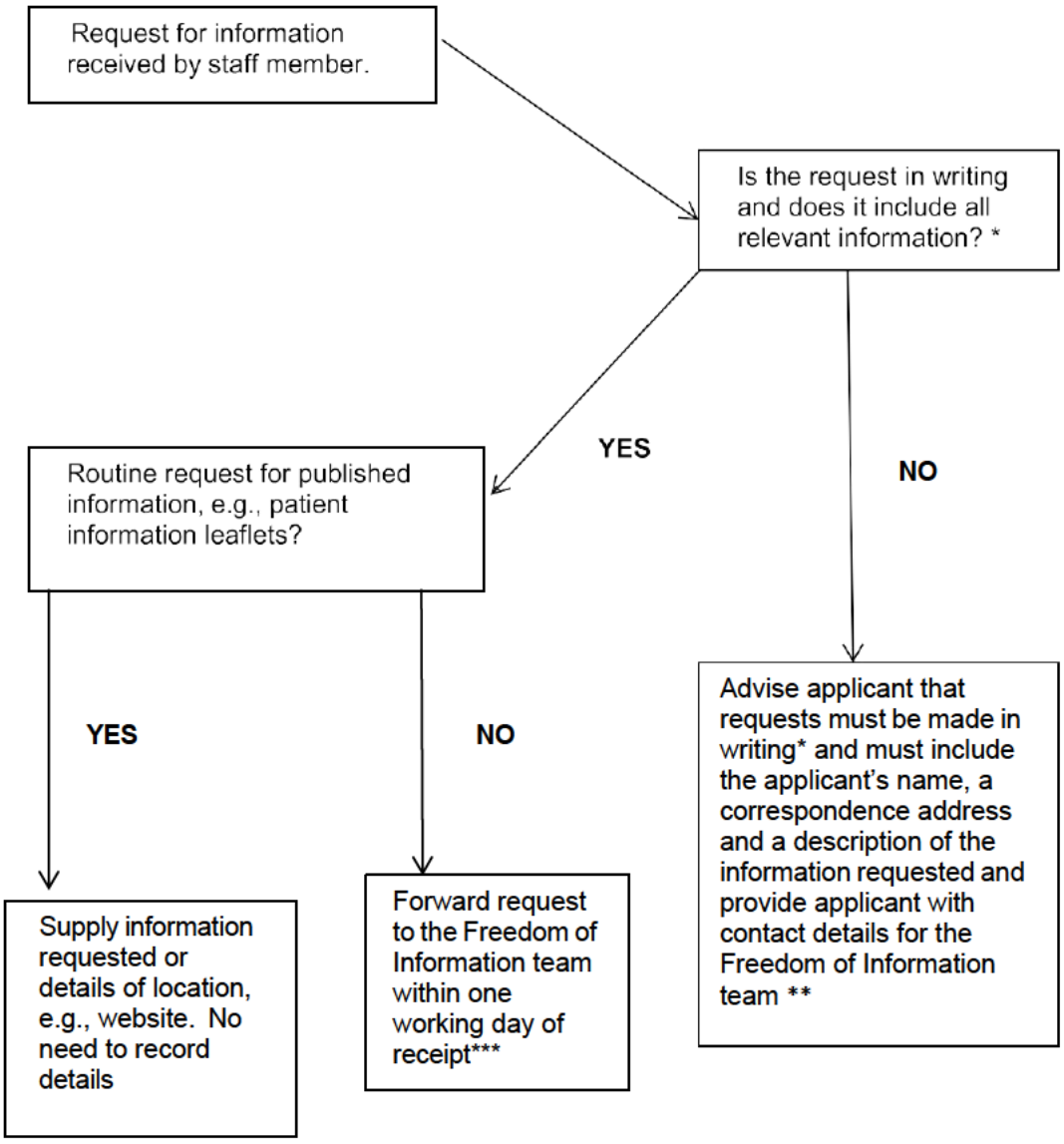


Figure 1

* Requests in writing may include e-mails, environmental information requests can be made verbally. All FOI and EIR requests must have the name of the applicant, a correspondence address and a description of the information requested.

** Freedom of Information Team, East Sussex Healthcare NHS Trust, Eastbourne DGH, Kings Drive, Eastbourne, East Sussex, BN21 2UD. Tel: 0300 131 4716 (internal 734716), E-mail: esh-tr.foi@nhs.net.

*** To save time, written requests should be scanned and e-mailed as soon as possible to the FOI inbox. Original documentation can then be sent on to follow.

NB. Although they are dealt with under the Freedom of Information Act, any requests for access to records of deceased patients should be forwarded immediately to the Request for Information Department, Eastbourne DGH, e-mail: esh-tr.sar@nhs.net.

6.3 Processing Requests for Information (see figure 2)

An acknowledgement will be sent within two working days to inform the applicant that their request has been received and is being processed.

The Freedom of Information team will review the request and contact the applicant for further information if this is necessary to process the application. They will also review the information in respect of possible exemptions and/or fees and seek advice from senior staff if required. In some circumstances this will only become apparent when passed to the relevant manager for a response.

The Freedom of Information team will inform the applicant if any charges or fees are applicable stating that no information will be provided unless the required fee or charge is paid within three months.

The details of the request for information will be entered onto the [redacted] database.

The Freedom of Information team will identify and contact the manager of the relevant department holding the information that the applicant has requested. Upon receipt of an FOI or EIR request, the manager has a total of **10 working days from the date the request was received by the Trust** to locate and provide the information requested to the Freedom of Information team. If it is not possible to meet this deadline, the team must be notified immediately.

Within **3 working days from the date the request was received by the Trust** the manager will need to confirm to the Freedom of Information team whether the information is held or not, or whether further searches are required in order to be able to confirm or deny.

As some requests may exceed the **appropriate cost limit (18 hours staff time or £450**), prior to processing the request the manager should assess the time reasonably expected to be required to:

- Determine whether the information is held.
- Locate the information, or a document containing it.
- Retrieve the information, or a document containing it; and
- Extract the information from a document containing it.

If it is likely that the cost limit will be exceeded, an estimate must be submitted in writing to the Freedom of Information team within **5 working days**, using the Justification Form – see Appendix C. This will then be used to enable the FOI Team to provide advice and assistance to the applicant in order to further refine their request.

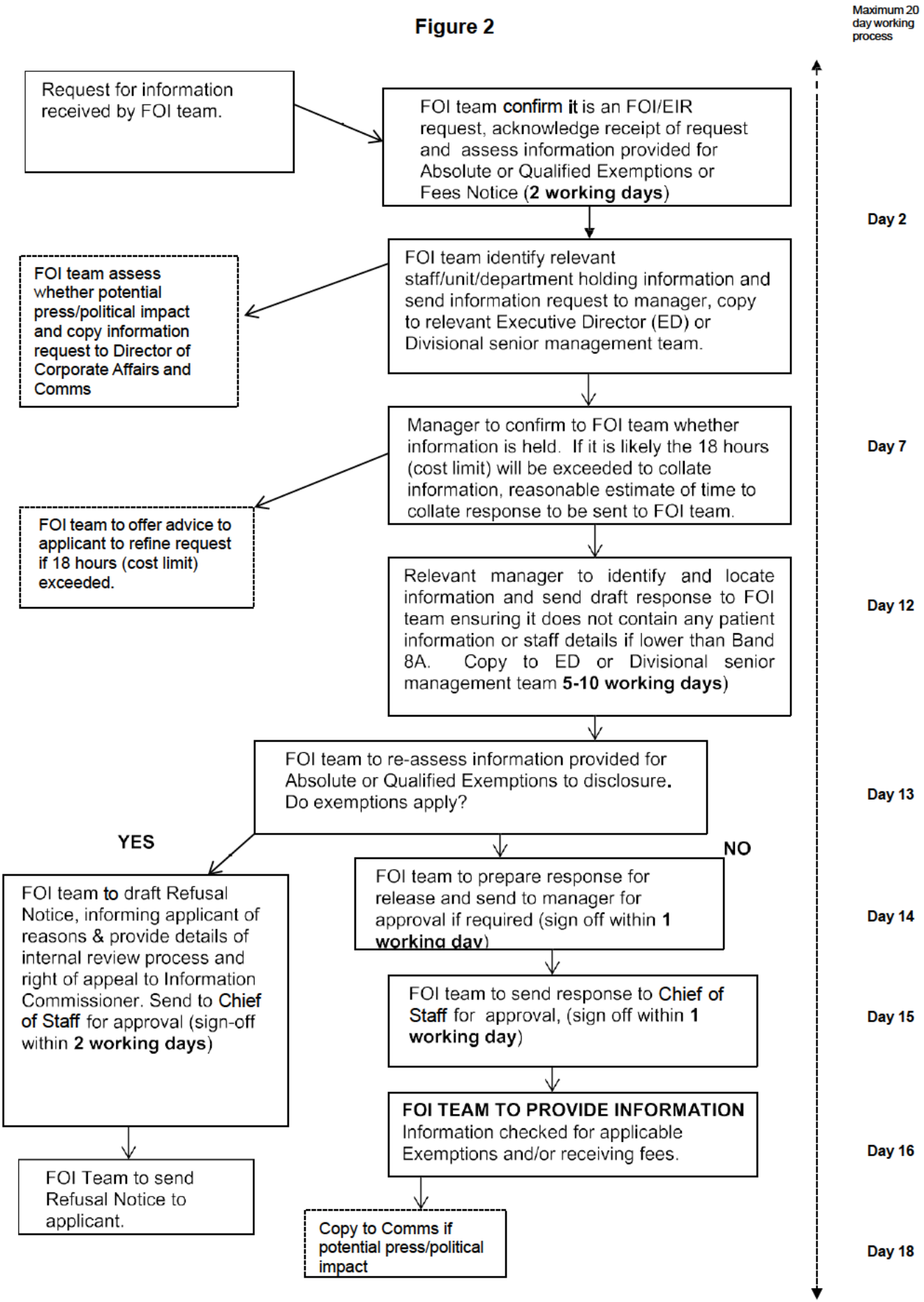
If the information is held, and the cost limit is not exceeded, the draft response and any associated attachments should be forwarded to the Freedom of Information team within the stated deadline. They will then further review the information in respect of exemptions and/or fees and seek advice from senior staff if required.

The Senior Freedom of Information Administrator and the team can provide advice on the FOI or EIR regulations to managers, but **managers must take ownership and responsibility for coordinating responses within statutory deadlines for requests which relate to their areas of work.**

The Freedom of Information team will draft the final response for sign-off by the Chief of Staff.

Once approved, the Freedom of Information Team will send out the response, copying it to the communications department if there is a potential press/political impact.

Figure 2


Maximum 20 day working process
Request for information received by FOI team.
FOI team confirm it is an FOI/EIR request, acknowledge receipt of request and assess information provided for Absolute or Qualified Exemptions or Fees Notice (2 working days)
Day 2
FOI team identify relevant staff/unit/department holding information and send information request to manager, copy to relevant Executive Director (ED) or Divisional senior management team.
FOI team assess whether potential press/political impact and copy information request to Director of Corporate Affairs and Comms
Manager to confirm to FOI team whether information is held. If it is likely the 18 hours (cost limit) will be exceeded to collate information, reasonable estimate of time to collate response to be sent to FOI team.
Day 7
FOI team to offer advice to applicant to refine request if 18 hours (cost limit) exceeded.
Relevant manager to identify and locate information and send draft response to FOI team ensuring it does not contain any patient information or staff details if lower than Band 8A. Copy to ED or Divisional senior management team 5-10 working days)
Day 12
FOI team to re-assess information provided for Absolute or Qualified Exemptions to disclosure. Do exemptions apply?
Day 13
YES
NO
FOI team to draft Refusal Notice, informing applicant of reasons & provide details of internal review process and right of appeal to Information Commissioner. Send to Chief of Staff for approval (sign-off within 2 working days)
FOI team to prepare response for release and send to manager for approval if required (sign off within 1 working day)
Day 14
FOI team to send response to Chief of Staff for approval, (sign off within 1 working day)
Day 15
FOI TEAM TO PROVIDE INFORMATION
Information checked for applicable Exemptions and/or receiving fees.
Day 16
FOI Team to send Refusal Notice to applicant.
Copy to Comms if potential press/political impact
Day 18

6.4 Providing the Information

Once the information has been reviewed and if no exemptions apply and if no charge or fee is payable, the Freedom of Information team will provide the information to the applicant.

If any charge or fee is payable, a fees notice will be issued to the applicant as soon as this is known, and the information will be released only when cleared payment is received.

Information will be provided to applicants by one or more of the following means, namely:

- As a **copy** of the information in permanent form or another form acceptable to the applicant.
- By providing the applicant with a reasonable opportunity to **inspect** a record containing the information.
- By providing a **digest or summary** of the information in permanent form or another form acceptable to the applicant.

Where a copy and/or a digest or summary is preferred and the information is to be made available electronically to the applicant, the electronic file shall be prepared and sent in a secure document format, i.e., Portable Document Form (PDF file), for reasons of integrity and security.

The Freedom of Information team will consider all the circumstances when providing information in a particular form, including the preferences stated in the original request and the practicalities. If the information being provided constitutes a data set and the requester has expressed a preference to receive the information in an electronic form, the public authority must provide it in a re-usable form so far as reasonably practicable.

The Re-Use of Public Sector Information Regulations (RoPSI) 2015 give the public and the private sector the right to re-use public sector information which the Trust produces as part of its Public Task. Re-using the information means to use it for a purpose other than the initial public task it was produced for. All requests for re-use under the RoPSI regulations must be made in writing (preferably by email), including a name and address for correspondence, specifying the information requested for re-use and the purpose it is intended to be used for. Where the Trust permits re-use of information under the Re-Use of Public Sector Information Regulations 2015 it is licensed under the Open Government License.

When making such decisions, the Freedom of Information team will have regard for other statutory obligations upon the Trust such as those established under the Equality Act 2010.