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

FOI REF: 26/063

13th March 2026

FREEDOM OF INFORMATION ACT

I am responding to your request for information under the Freedom of Information Act. The answers to your specific questions are as follows:

Under the Freedom of Information Act 2000, I would be grateful if you could provide the information requested below in relation to your Cellular Pathology service.

Clarification was sought with regard to your definition of Locum, i.e. do you mean Agency and confirmation was received as follows:

Yes, it will be agency.

1. Case Volumes & Activity

1.1 Total number of Cellular Pathology cases processed:

- **In the most recent completed financial year**

  35,203

- **Year-to-date for the current financial year**

  25,972

1.2 Average monthly case volume.

2,886

2. Current Backlog & Turnaround Times

2.1 Current number of unreported cases, broken down by:

- **Routine**

  0.

- **Urgent / cancer**

  0.

The information requested above can only be provided at a fixed point in time, therefore the figures above are for the end of December 2025.

2.2 Backlog volume by sub-specialty (e.g. GI, Gynaecological, Breast, Skin, Urology, etc.).

0.

2.3 Average turnaround times (TATs) for:

The figures provided below are for December 2025.

- **Routine cases**

  52% in ten days.

- **Urgent / cancer cases**

  52% in ten days.

2.4 Highest backlog volume recorded in the past 12 months.

There is no backlog, as there are measures in place.

3. Backlog Management Measures

Please confirm which of the following measures are currently used to manage reporting backlogs (and specify where applicable):

- **Consultant overtime / internal insourcing**

  Consultants do report additional cases as part of a work list initiative, as and when required.

- **Use of locum consultant pathologists**

  There are no agency consultant pathologists in place.

- **Outsourcing to external reporting providers**

  The Trust uses external companies for reporting.

- **Digital pathology / remote reporting**

  The Trust uses external companies for reporting.

- **Other measures (please specify)**

  The Trust are using Insourcing for laboratory capacity.

4. Outsourcing & Locum Spend (Last 3 Financial Years)

4.1 Outsourced Reporting

For each of the last three financial years, please provide:

a. Total spend on outsourced pathology reporting.

2022/23	£1,000,374
2023/24	£1,859,058
2024/25	£2,108,646

b. Number of cases outsourced.

2022/23	15,336
2023/24	16,076
2024/25	18,794

c. Names of external reporting providers used.

LDPath / Source BioScience and Diagnexia.

d. Whether service level agreements (SLAs) are in place and, if so:

Yes, these are in place.

- **Agreed turnaround times**

  Yes, these are in place.

- **Any performance measures or penalties (if applicable)**

  Yes, these are in place.

4.2 Locum & Agency Spend

a. Total spend on locum consultant pathologists.

0.

b. Names of agencies used.

Not applicable.

c. Average duration of locum engagements.

Not applicable.

5. Digital Pathology Infrastructure

5.1 Whether digital pathology is currently used for primary diagnosis (Yes/No).

Yes.

5.2 If yes:

o Manufacturer and model of whole-slide scanners in use

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 for questions 5.1 and 5.2 is being withheld. 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.

- **Year digital pathology reporting commenced**

  2023

- **Whether remote reporting is enabled**

  Yes.

5.3 Current Laboratory Information Management System (LIMS).

Section 31(1)(a) applied, please refer to question 5.2.

5.4 Approximate percentage of cases currently reported digitally.

86% (as at December 2025).

6. Workforce Capacity

6.1 Current establishment (WTE) of:

- **Substantive consultant pathologists**

  9.9 WTE.

- **Biomedical Scientists / Advanced Practitioners**

  87.1 WTE.

6.2 Number of additional consultants and BMS staff required to operate at full service capacity.

No demand and capacity information is available.

6.3 Sub-specialties where staffing shortages are most acute.

Head & Neck, Lymphoma and Gynaecology.

7. Future Planning

7.1 Whether the Trust has a documented strategy or business case for:

- **Expanding digital pathology**

  No, as this is already in place.

- **Increasing remote reporting capability**

  The aim is to reduce reliance on outsourcing reporting capacity.

- **Reducing backlogs through external or hybrid support models**

  The aim is to manage demand internally.

7.2 Indicative timelines for implementation within the next 12–24 months (if available).

Not applicable.

8. Relevant Contacts & Engagement

8.1 Please provide the name, job title, and work contact details (email address and telephone number) for the following roles:

- **Laboratory Manager / Head of Cellular Pathology**

  Ellie Hopkins-Button (Lead Biomedical Scientist – Histology).

- **Lead Consultant Pathologist**

  Dr Zainab Ali (Consultant – Histopathology).

- **Clinical Director for Pathology or Diagnostics**

  Dr David Till (Consultant Endocrinologist and Chief of Core Services).

We are unable to provide the contact details of staff as we consider this information to be exempt from release in accordance with section 44 of the Freedom of Information Act (Prohibition on disclosure) and would refer to the Privacy and Electronic Communications EC Directive Regulations 2003 which provide specific rules on electronic communication services, including marketing (by phone, fax, email or text) and keeping communications services secure. We will not provide any information that could result in the transmission of unsolicited communications which may place an unacceptable risk to our email

network and could also have a detrimental impact on patient care and treatment.

The contact number for the Trust is accessible on the Trust website http://www.esht.nhs.uk.

This is an absolute exemption and there is, therefore, no requirement to consider the public interest.

8.2 Please confirm whether the Trust would be open to a conversation regarding potential solutions to support:

- **Backlog reduction**

  No, as the Cellular Pathology team will engage with the market via the Trust's procurement procedures.

- **Workforce capacity constraints**

  No, as the Cellular Pathology team will engage with the market via the Trust's procurement procedures.

- **Digital pathology or remote reporting initiatives**

  No, as the Cellular Pathology team will engage with the market via the Trust's procurement procedures.

8.3 If so, please confirm the most appropriate individual or department to contact for such discussions.

Esht.procurement@nhs.net.

9. Cancer Pathway Performance

9.1 Please confirm whether the Trust has breached national cancer waiting time targets (e.g. the 62-day cancer pathway) due to Cellular Pathology reporting delays within the last 12 months.

East Sussex Healthcare NHS Trust does not centrally record this information. To enable the Trust to provide this information would require a manual review of all patient episodes that have breached cancer waiting time targets, which we estimate would take over 70 hours. This is because all breaches are recorded in granular detail and a year's worth of data would need to be reviewed manually to establish whether or not Cellular Pathology reporting delays were the principle cause of any breaches. We are therefore applying Section 12(1) to this part of your request.

Section 12(1) of the Act allows a public authority to refuse to comply with a request for information if the authority estimates that the cost of compliance would exceed the 'appropriate limit', as defined by the Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004 (the

Regulations). These state that this cost limit is £450 for public authorities which are not part of central government or the armed forces. The costs are calculated at £25 per hour per person regardless of the rate of pay, which means that the limit will be exceeded if the work involved would exceed 18 hours. The Trust estimates that the cost of complying with this request would significantly exceed the above limit.

9.2 If yes, please provide the number of cases affected (where available).

Please see the response to Q9.1

10. Glass Slide Handling

10.1 Whether physical glass slides are currently transported off-site for external reporting (Yes/No).

Yes.

10.2 If yes:

- **Approximate monthly volume of cases**

  The Trust does not record this information.

- **Method of transport (e.g. courier, internal transfer)**

  Courier.

11. Consultant Reporting Capacity

11.1 Whether current consultant pathologists are reporting at full programmed activity capacity (Yes/No).

Yes.

11.2 If no, please outline the main limiting factors (e.g. job planning constraints, SPA commitments, management duties).

Not applicable.

12. Governance & Access Constraints

12.1 Please confirm whether there are any governance, IT, or information governance restrictions that limit the use of:

- **External reporters**

  Yes.

- **Remote digital pathology reporting**

  Yes.

12.2 If yes, please outline the nature of these restrictions.

They must be UKAS accredited, follow screening guidance, meet DPIA (Data Protection Impact Assessment) , partake in EQA (External Equality Assessments), partake in audit to show compliance and report to RCPath (Royal College of Pathologists) reporting standards

13. Backlog Mitigation Models Used

13.1 Please confirm which of the following backlog mitigation models the Trust has utilised within the last 12 months:

- **On-site agency locum consultant pathologists**

  No.

- **Off-site outsourced reporting (digital and/or glass slides)**

  Yes.

- **Hybrid models (combination of on-site and off-site support)**

  Yes.

13.2 Where more than one model has been used, please confirm whether:

- **One model has been used more frequently than the others, or**

  The Trust's own capacity is used first, followed by digital outsourcing.

- **Usage has been broadly equivalent.**

  It varies, depending on in-house capacity.

13.3 Please confirm whether any internal policy, guidance, or procurement preference exists regarding:

- **On-site agency locums versus**

  There is a requirement nationally to control this spend.

- **Outsourced / off-site reporting solutions.**

  No internal policy, guidance or preference exists, but it is deemed more controlled due to the competitive process and having contracts with Terms & Conditions and Key Performance Indicators in place.

If I can be of any further assistance, please do not hesitate to contact me.

Should you be dissatisfied with the Trust's response to your request, you have the right to request an internal review. Please write to the Freedom of Information Department (esh-tr.foi@nhs.net), quoting the above reference, within 40 working days. The Trust is not obliged to accept an internal review after this date.

Should you still be dissatisfied with your FOI request, you have the right of complaint to the Information Commissioner at the following address:

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

Telephone: 0303 123 1113

Yours sincerely

Freedom of Information Department
esh-tr.foi@nhs.net