

FOI 3631

10th March 2026

FREEDOM OF INFORMATION ACT 2000 – INFORMATION REQUEST

1. Please provide the record from the organisation's Contract Register or equivalent procurement log entry pertaining to the current contract for the Endpoint Detection and Response (EDR) solution (Include Supplier, Product Name, Start Date, Expiry Date, Annual spend 2025/2026 [£], Additional notes [including any framework used])

🔍 DEFINITION: The practice of securing organisational assets such as laptops, desktops, mobile phones, and servers against malicious activity. It encompasses tools and strategies designed to detect, prevent, and respond to threats directly on the device itself.

Response:

The information requested is exempt from release under Section 31 and Section 43 of the Freedom of Information Act 2000.

These are both qualified exemptions and so a Public Interest Test was carried out to decide if the information should be released or not. Having weighed up the factors for and against release, it was decided to withhold this information because the disclosure of such information would:

- a) Leave (Southern Health & Social Care Trust) patients, clients & staff more vulnerable to crime (Section 31)
- b) Pose a significant threat to the integrity & operation of the digital systems on which the day-to-day business of the (Southern Health & Social Care Trust) relies (Section 43).

Section 31 – Law Enforcement Section

Section 31(1)(a) states that information is exempt if its disclosure is likely to prejudice the prevention or detection of crime. ICO guidance states that this can be used to protect information on a public authority's systems which would make it more vulnerable to crime. It can be used by a public authority that has no law enforcement function:

* To protect the work of one that does

* To withhold information that would make anyone, including the public authority itself, more vulnerable to crime.

2. Please provide the following information for the current maintenance and licensing agreement for the primary Perimeter Firewall/Intrusion Prevention System (IPS) solution (Include Supplier, Product Name, Start Date, Expiry Date, Annual spend 2025/2026 [£], Additional notes [including any framework used])

🔍 DEFINITION: The processes and technologies used to protect the boundaries (the perimeter) of an organisation's internal network from unauthorised external access. It involves monitoring and controlling incoming and outgoing network traffic.

Response:

The information requested is exempt from release under Section 31 and Section 43 of the Freedom of Information Act 2000.

These are both qualified exemptions and so a Public Interest Test was carried out to decide if the information should be released or not. Having weighed up the factors for and against release, it was decided to withhold this information because the disclosure of such information would:

- a) Leave (Southern Health & Social Care Trust) patients, clients & staff more vulnerable to crime (Section 31)
- b) Pose a significant threat to the integrity & operation of the digital systems on which the day-to-day business of the (Southern Health & Social Care Trust) relies (Section 43).

Section 31 – Law Enforcement Section

Section 31(1)(a) states that information is exempt if its disclosure is likely to prejudice the prevention or detection of crime. ICO guidance states that this can be used to protect information on a public authority's systems which would make it more vulnerable to crime. It can be used by a public authority that has no law enforcement function:

- * To protect the work of one that does
- * To withhold information that would make anyone, including the public authority itself, more vulnerable to crime.

3. Please provide the following information for the service agreement covering the Cloud Security Posture Management (CSPM) platform or equivalent third-party cloud security monitoring too (Include Supplier, Product Name, Start Date, Expiry Date, Annual spend 2025/2026 [£], Additional notes [including any framework used])

DEFINITION: The set of security measures designed to protect data, applications, and infrastructure running in cloud environments (e.g., AWS, Azure, GCP). It also includes securing internally and externally facing applications themselves (application security).

Response:

The information requested is exempt from release under Section 31 and Section 43 of the Freedom of Information Act 2000.

These are both qualified exemptions and so a Public Interest Test was carried out to decide if the information should be released or not. Having weighed up the factors for and against release, it was decided to withhold this information because the disclosure of such information would:

- a) Leave (Southern Health & Social Care Trust) patients, clients & staff more vulnerable to crime (Section 31)
- b) Pose a significant threat to the integrity & operation of the digital systems on which the day-to-day business of the (Southern Health & Social Care Trust) relies (Section 43).

Section 31 – Law Enforcement Section

Section 31(1)(a) states that information is exempt if its disclosure is likely to prejudice the prevention or detection of crime. ICO guidance states that this can be used to protect information on a public authority's systems which would make it more vulnerable to crime. It can be used by a public authority that has no law enforcement function:

- * To protect the work of one that does

* To withhold information that would make anyone, including the public authority itself, more vulnerable to crime.

4. Please provide the following information for the service agreement covering your Identity & Access Management (IAM) software (Include Supplier, Product Name, Start Date, Expiry Date, Annual spend 2025/2026 [£], Additional notes [including any framework used])

🔍 DEFINITION: A framework of policies and technologies that ensures the right users have the appropriate access to the right resources at the right time. It involves managing digital identities, authentication (verifying identity), and authorisation (granting access).

Response:

The information requested is exempt from release under Section 31 and Section 43 of the Freedom of Information Act 2000.

These are both qualified exemptions and so a Public Interest Test was carried out to decide if the information should be released or not. Having weighed up the factors for and against release, it was decided to withhold this information because the disclosure of such information would:

- a) Leave (Southern Health & Social Care Trust) patients, clients & staff more vulnerable to crime (Section 31)
- b) Pose a significant threat to the integrity & operation of the digital systems on which the day-to-day business of the (Southern Health & Social Care Trust) relies (Section 43).

Section 31 – Law Enforcement Section

Section 31(1)(a) states that information is exempt if its disclosure is likely to prejudice the prevention or detection of crime. ICO guidance states that this can be used to protect information on a public authority's systems which would make it more vulnerable to crime. It can be used by a public authority that has no law enforcement function:

* To protect the work of one that does

* To withhold information that would make anyone, including the public authority itself, more vulnerable to crime.

5. Please provide the record from the organisation's Contract Register or equivalent procurement log entry pertaining to the current contract for your current Managed Security / SOC Services (Include Supplier, Product Name, Start Date, Expiry Date, Annual spend 2025/2026 [£], Additional notes [including any framework used])

🔍 DEFINITION: The outsourcing of security monitoring and management to a third-party expert. A Security Operations Center (SOC) is a centralised function (internal or outsourced) responsible for continuous monitoring, threat analysis, and managing security incidents.

Response:

The information requested is exempt from release under Section 31 and Section 43 of the Freedom of Information Act 2000.

These are both qualified exemptions and so a Public Interest Test was carried out to decide if the information should be released or not. Having weighed up the factors for

and against release, it was decided to withhold this information because the disclosure of such information would:

- a) Leave (Southern Health & Social Care Trust) patients, clients & staff more vulnerable to crime (Section 31)
- b) Pose a significant threat to the integrity & operation of the digital systems on which the day-to-day business of the (Southern Health & Social Care Trust) relies (Section 43).

Section 31 – Law Enforcement Section

Section 31(1)(a) states that information is exempt if its disclosure is likely to prejudice the prevention or detection of crime. ICO guidance states that this can be used to protect information on a public authority's systems which would make it more vulnerable to crime. It can be used by a public authority that has no law enforcement function:

* To protect the work of one that does

* To withhold information that would make anyone, including the public authority itself, more vulnerable to crime.

6. Please provide the record from the organisation's Contract Register or equivalent procurement log entry pertaining to the current contract for your current Vulnerability & Compliance Management service (Include Supplier, Product Name, Start Date, Expiry Date, Annual spend 2025/2026 [£], Additional notes [including any framework used])

2 DEFINITION: The continuous, cyclical practice of identifying, classifying, prioritising, remediating, and mitigating software weaknesses (vulnerabilities). Compliance Management ensures that security practices adhere to specific internal policies, regulatory requirements (like GDPR), and industry standards.

Response:

The information requested is exempt from release under Section 31 and Section 43 of the Freedom of Information Act 2000.

These are both qualified exemptions and so a Public Interest Test was carried out to decide if the information should be released or not. Having weighed up the factors for and against release, it was decided to withhold this information because the disclosure of such information would:

- a) Leave (Southern Health & Social Care Trust) patients, clients & staff more vulnerable to crime (Section 31)
- b) Pose a significant threat to the integrity & operation of the digital systems on which the day-to-day business of the (Southern Health & Social Care Trust) relies (Section 43).

Section 31 – Law Enforcement Section

Section 31(1)(a) states that information is exempt if its disclosure is likely to prejudice the prevention or detection of crime. ICO guidance states that this can be used to protect information on a public authority's systems which would make it more vulnerable to crime. It can be used by a public authority that has no law enforcement function:

* To protect the work of one that does

* To withhold information that would make anyone, including the public authority itself, more vulnerable to crime.

Email: foi.team@southerntrust.hscni.net