NHS Borders
Planning & Performance

NHS Borders
Education Centre
Borders General Hospital
Melrose
Roxburghshire
TD6 9BD
01896 825545
foi.enquiries@borders.scot.nhs.uk

Freedom of Information request 77-21

Request

1. Who is the current provider for the trusts network infrastructure? - When considering network infrastructure this is specifically the switching hardware and wireless access points that may be deployed throughout the trusts estate and associated cabling etc.
2. How many sites does the trust have responsibility for that require a network infrastructure as detailed above?
3. What manufacturer does the trust use for the above-mentioned network infrastructure?
4. What are the approximate number of network switches deployed throughout the estate?
5. What are the approximate number of wireless access points deployed across the estate?
6. What is the latest Wi-Fi version the trust support i.e. 802.11 b/g/n/ac/ax
7. Does the trust provide public Wi-Fi access via its network infrastructure and wireless access points it has deployed?
8. How often does the trust refresh the deployed network infrastructure?
9. When do the existing contracts for the switching network and wireless network expire?
10. What vendor currently provides the trust's cyber security system?
11. How many users utilise the cyber security solution?
12. How often does the cyber security solution get refreshed or upgraded?
13. Who provides the current cyber security solution? I.e. is this direct with the software company or through a partner?
14. When do the existing contracts for the current cyber security solution expire?
15. How does the trust purchase new hardware is this via a standard industry framework agreement or directly to the market via an open tendering process?
16. Does the trust have a fully defined IT strategy?
17. If the answer to question 10 is yes can a copy be provided?
18. Can the trust provide a copy of the IT departments organisational chart or if not available a list of the names and roles of those people that work in it.
19. Finally, can the trust confirm if the IT department make the final decisions with regards to purchasing new solutions for the IT environment.

Response

1. This is managed internally by the IM&T Service.

2. There are 37 locations.

3. We are withholding this information under Section 24 (1) (National Security) of the Freedom of Information Act and Section 31(1) (a) of the Act (law enforcement) which covers all aspects of the prevention and detection of crime. Both section 24 and 31 are qualified exemptions,which means they are subject to a public interest test. Under Section 24 (1) we consider that disclosure would not be in the interest of the Boards' security. Disclosing details about operating systems and e-mail security systems could allow individuals to assess the strength of our defences. The public interest arguments against disclosure under Section 31 (1) (a) are similar. Any attempt to hack into an IT system is a criminal offence. Disclosing this information could aid, and indeed encourage, a criminal who was intent on launching an attack on the Department's ICT systems and could expose the Board to potential threats such as targeted e-crime. We acknowledge the public interest in openness and transparency. We also appreciate that disclosure of this information would provide information on the scale of threat posed by cyber attacks. However, for the reasons outlined we have concluded that thebalance of public interest favours withholding this information.

4. There are approx 300 network switches.

5. There are approx 350 wireless access points deployed.

6. 802.11 b/g/n

7. Public WiFi is provided through the organisational network infrastructure on the main BGH campus.

8. Every 5-7 Years

9. Support & Maintenance Contracts end in December 2023.

10. We are withholding this information under Section 24 (1) (National Security) of the Freedom of Information Act and Section 31(1) (a) of the Act (law enforcement) which covers all aspects of the prevention and detection of crime. Both section 24 and 31 are qualified exemptions, which means they are subject to a public interest test. Under Section 24 (1) we consider that disclosure would not be in the interest of the Boards' security. Disclosing details about operating systems and e-mail security systems could allow individuals to assess the strength of our defences. The public interest arguments against disclosure under Section 31 (1) (a) are similar. Any attempt to hack into an IT system is a criminal offence. Disclosing this information could aid, and indeed encourage, a criminal who was intent on launching an attack on the Department's ICT systems and could expose the Board to potential threats such as targeted e-crime. We acknowledge the public interest in openness and transparency. We also appreciate that disclosure of this information would provide information on the scale of threat posed by cyber attacks. However, for the reasons outlined we have concluded that the balance of public interest favours withholding this information.

11. 3700

12. A review is carried out every 3 years and upgrades carried out in line with supplier recommendations.

13. We are withholding this information under Section 24 (1) (National Security) of the Freedom of Information Act and Section 31(1) (a) of the Act (law enforcement) which covers all aspects of the prevention and detection of crime. Both section 24 and 31 are qualified exemptions, which means they are subject to a public interest test. Under Section 24 (1) we consider that disclosure would not be in the interest of the Boards' security. Disclosing details about operating systems and e-mail security systems could allow individuals to assess the strength of our defences. The public interest arguments against disclosure under Section 31 (1) (a) are similar. Any attempt to hack into an IT system is a criminal offence. Disclosing this information could aid, and indeed encourage, a criminal who was intent on launching an attack on the Department's ICT systems and could expose the Board to potential threats such as targeted e-crime. We acknowledge the public interest in openness and transparency. We also appreciate that disclosure of this information would provide information on the scale of threat posed by cyber attacks. However, for the reasons outlined we have concluded that the balance of public interest favours withholding this information.

14. January 2026

15. National Framework Agreements

16. NHS Borders has an existing strategy that is coming to end of life and a review is currently taking place.

17. Please find attached a copy of the existing strategy:

    Road To Digital.pdf

18. Please find attached a copy of the IM&T structure chart:

    IM&T Structure Chart 120820 (no na

19. All local requirements are decided by the NHS Borders IT Management team with support from the NHS Board. There are National systems and solution which are provided centrally in collaboration with the territorial boards.

If you are not satisfied with the way your request has been handled or the decision given, you may ask NHS Borders to review its actions and the decision. If you would like to request a review please apply in writing to, Freedom of Information Review, NHS Borders, Room 2EC3, Education Centre, Borders General Hospital, Melrose, TD6 9BS or foi.enquiries@borders.scot.nhs.uk.

The request for a review should include your name and address for correspondence, the request for information to which the request relates and the issue which you wish to be reviewed. Please state the reference number **77-21** on this request. Your request should be made within 40 working days from receipt of this letter.

If following this review, you remain dissatisfied with the outcome, you may appeal to the Scottish Information Commissioner and request an investigation of your complaint. Your request to the Scottish Information Commissioner should be in writing (or other permanent form), stating your name and an address for correspondence. You should provide the details of the request and your reasons for dissatisfaction with both the original response by NHS Borders and your reasons for dissatisfaction with the outcome of the internal review. Your application for an investigation by the Scottish Information Commissioner must be made within six months of your receipt of the response with which you are dissatisfied. The address for the Office of the Scottish Information Commissioner is, Office of the Scottish Information Commissioner, Kinburn Castle, Doubledykes Road, St Andrews, Fife.