NHS
Kent and Medway
NHS and Social Care Partnership Trust
Information Governance & Records Management Department
St Michaels House
St Michaels Road
Sittingbourne
Kent
ME10 3DW

Tel: 01795 514525

Email: kmpt.inforaccess@nhs.net
Website: www.kmpt.nhs.uk

Sent via email

Dear [redacted],

Request for Information

I write further to your request FOI ID 1790 under the Freedom of Information Act 2000 regarding: -

Back up and Data Protection

Your request is set out below:

1. How much data do you store operationally?

   287,667 GiB

2. What is your organisation's current data recovery process?

   The Trust has carried out a Public Interest Test and information relating to the Trust's Data Recovery process will not be released. We are applying exemptions:

   31(1)(a) as releasing the information may result in criminal activity,
   31(1)(g) may impact the ability for the Trust to undertake its daily functions.,
   31(2)((i)(j)) May expose staff to risk to their health and safety,
   38(1)(a) and 38(1)(b) Such actions would endanger the physical health and safety of an individual should the Trust not be able to access health records and results electronically.

3. How often does your organisation perform backups of critical data, and is this an automatic or manual backup?

   The trust takes a full back up weekly and daily incrementals all fully automated.

4. Which data backup solutions does your organisation currently employ?

   The Trust has carried out a Public Interest Test and information relating to the Trust's Data Backup Solutions will not be released. We are applying exemptions:

31(1)(a) as releasing the information may result in criminal activity,
31(1)(g) may impact the ability for the Trust to undertake its daily functions.,
31(2)((i)(j)) May expose staff to risk to their health and safety,
38(1)(a) and 38(1)(b) Such actions would endanger the physical health and safety of an individual should the Trust not be able to access health records and results electronically.

5. What is the average recovery time for your organisation in event of failure or data loss?

   The Trust has carried out a Public Interest Test and information relating to the Trust's Data Backup Solutions will not be released. We are applying exemptions:

   31(1)(a) as releasing the information may result in criminal activity,
   31(1)(g) may impact the ability for the Trust to undertake its daily functions.,
   31(2)((i)(j)) May expose staff to risk to their health and safety,
   38(1)(a) and 38(1)(b) Such actions would endanger the physical health and safety of an individual should the Trust not be able to access health records and results electronically.

6. Does your organisation have a formalised disaster recovery plan?

   Yes

7. How often does your organisation test the effectiveness of its disaster recovery plan?

   Annually

8. What types of disasters or incidents does your disaster recovery plan cover?

   All types of known incidents are included within the Trusts Emergency Planning Readiness Response planning.

9. Has your organisation experienced any significant data loss incidents in the past two years? If so, how were they addressed?

   No

10. How does your organisation handle the storage and management of backup tapes or other physical backup media?

    N/A

11. Does your organisation utilise virtualisation technology for any critical systems or applications?

    Yes, where these fit with supplier best practice and published guidelines

12. Are there any specific challenges or pain points that your organisations faces regarding VMware or virtualisation technology?

    No

13. How frequently does your organisation update or upgrade its Virtualisation software?

    Updates are released, tested and applied when released by the vendor

14. What backup/recovery solutions does your organisation use for virtual machines?

    The same technology is used as for data

15. Has your organisation have any plans to migrate away from legacy backup or disaster recovery systems? If yes, what is the timeline for migration?

    A new solution has already been procured and is currently in planning for replacement by December 2023.

16. How does your organisation ensure the security and confidentiality of backup data during transmission and storage?

    Security measures in place include firewalls, encryption in transit and at rest, offline/offsite copies. To provide detail this would present a significant security risk by revealing details of the trusts information system security.

17. Are there any legal or compliance requirements that impact your organisation's data recovery/backup/disaster recovery processes?

    The trust must meet NHS and public sector data retention requirements.

18. When are your contracts for Data Recovery, Backup, Disaster Recovery and VMware related initiatives up for renewal, please express in bullet points and indicate if supplied by multiple vendors or single vendor

    The data back up solution for the Trust has just been renewed and will expire in December 2026.

I confirm that the information above completes your request under the Freedom of Information Act 2000. I am also pleased to confirm that no charge will be made for this request.

If you have any questions or concerns or are unhappy with the response provided or the service you have received you can write to the Head of Information Governance at the address on top of this letter. If you are not content with the outcome of your complaint, you may apply directly to the Information Commissioner for a decision.

Yours Sincerely

On Behalf of
The Information Governance Department