

1. What is your annual IT Budget for 2017, 2018 & 2019?

For supplies and services the annual revenue budgets are:

2017	2018	2019
£104,600.00	£99,118.00	£102,800.00

2. Storage:

a. What storage vendor(s) and models do you currently use?

The information requested is covered by the exemptions (23) in Part II of the Freedom of Information Act.

The exemptions relate to security information, and is based on the harm that would arise or would be likely arise from disclosure.

To decide whether disclosure (or confirmation/denial) would cause prejudice we have undertaken the following: Prejudice test

- We are able to identify a negative consequence of the disclosure (or confirmation/denial), and this negative consequence is significant (more than trivial): Exploitation information would allow the propagation and enablement of vulnerability toolkits to attack the network.
- We are able to show a link between the disclosure (or confirmation/denial) and the negative consequences, thus us showing information on attack types and confirmation or denial on data loss would identify vulnerability's that would cause targeted attacks of that type.
- Currently there is a real possibility of the negative consequences happening, the release of this information is more likely than not to provide a targeted attack platform for exploitation.

b. What is the capacity of the storage data in TB & how much of this is utilised?

- One (Total 38Tb Used 27Tb)
- Two (Total 44Tb Used 20Tb)
- Three (Total 160TB Used 105TB)

c. What were the installation dates of the above storage vendor(s)? (Month/Year)

- January 2018
- June 2012
- August 2014

d. When is your planned (or estimated) storage refresh date? (Month/Year)?

- 2021

e. Do you have any extended warranties, if so, with which supplier?

- No

f. What is your estimated budget for the storage refresh?

- £180,000 including servers

3. Server/Compute:

a. What server vendor(s) and models do you currently use?

The information requested is covered by the exemptions (23) in Part II of the Freedom of Information Act.

The exemptions relate to security information, and is based on the harm that would arise or would be likely arise from disclosure.

To decide whether disclosure (or confirmation/denial) would cause prejudice we have undertaken the following: Prejudice test

- We are able to identify a negative consequence of the disclosure (or confirmation/denial), and this negative consequence is significant (more than trivial): Exploitation information would allow the propagation and enablement of vulnerability toolkits to attack the network.
- We are able to show a link between the disclosure (or confirmation/denial) and the negative consequences, thus us showing information on attack types and confirmation or denial on data loss would identify vulnerability's that would cause targeted attacks of that type.
- Currently there is a real possibility of the negative consequences happening, the release of this information is more likely than not to provide a targeted attack platform for exploitation.

b. What were the installation dates of the above server vendor(s)? (Month/Year)

- June 2012
- January 2018

c. When is your planned (or estimated) server refresh date? (Month/Year)

- 10/2021

d. What is your estimated budget for the server refresh?

- £180,000 including storage

e. Do you have any extended warranties, if so, with which supplier?

- Yes

The information requested is covered by the exemptions (23) in Part II of the Freedom of Information Act.

The exemptions relate to security information, and is based on the harm that would arise or would be likely arise from disclosure.

To decide whether disclosure (or confirmation/denial) would cause prejudice we have undertaken the following: Prejudice test

- We are able to identify a negative consequence of the disclosure (or confirmation/denial), and this negative consequence is significant (more than trivial): Exploitation information would allow the propagation and enablement of vulnerability toolkits to attack the network.

- We are able to show a link between the disclosure (or confirmation/denial) and the negative consequences, thus us showing information on attack types and confirmation or denial on data loss would identify vulnerability's that would cause targeted attacks of that type.
- Currently there is a real possibility of the negative consequences happening, the release of this information is more likely than not to provide a targeted attack platform for exploitation.

f. Which operating systems are used?

The information requested is covered by the exemptions (23) in Part II of the Freedom of Information Act.

The exemptions relate to security information, and is based on the harm that would arise or would be likely arise from disclosure.

To decide whether disclosure (or confirmation/denial) would cause prejudice we have undertaken the following: Prejudice test

- We are able to identify a negative consequence of the disclosure (or confirmation/denial), and this negative consequence is significant (more than trivial): Exploitation information would allow the propagation and enablement of vulnerability toolkits to attack the network.
- We are able to show a link between the disclosure (or confirmation/denial) and the negative consequences, thus us showing information on attack types and confirmation or denial on data loss would identify vulnerability's that would cause targeted attacks of that type.
- Currently there is a real possibility of the negative consequences happening, the release of this information is more likely than not to provide a targeted attack platform for exploitation.

4. Network & Security:

a. What network vendor(s) and models do you currently use?

The information requested is covered by the exemptions (23) in Part II of the Freedom of Information Act.

The exemptions relate to security information, and is based on the harm that would arise or would be likely arise from disclosure.

To decide whether disclosure (or confirmation/denial) would cause prejudice we have undertaken the following: Prejudice test

- We are able to identify a negative consequence of the disclosure (or confirmation/denial), and this negative consequence is significant (more than trivial): Exploitation information would allow the propagation and enablement of vulnerability toolkits to attack the network.
- We are able to show a link between the disclosure (or confirmation/denial) and the negative consequences, thus us showing information on attack types and confirmation or denial on data loss would identify vulnerability's that would cause targeted attacks of that type.
- Currently there is a real possibility of the negative consequences happening, the release of this information is more likely than not to provide a targeted attack platform for exploitation.

b. What are the quantities of the Edge, Core and MP used in your network?

- None

c. What network architecture is currently used?

The information requested is covered by the exemptions (23) in Part II of the Freedom of Information Act.

The exemptions relate to security information, and is based on the harm that would arise or would be likely arise from disclosure.

To decide whether disclosure (or confirmation/denial) would cause prejudice we have undertaken the following: Prejudice test

- We are able to identify a negative consequence of the disclosure (or confirmation/denial), and this negative consequence is significant (more than trivial): Exploitation information would allow the propagation and enablement of vulnerability toolkits to attack the network.
- We are able to show a link between the disclosure (or confirmation/denial) and the negative consequences, thus us showing information on attack types and confirmation or denial on data loss would identify vulnerability's that would cause targeted attacks of that type.
- Currently there is a real possibility of the negative consequences happening, the release of this information is more likely than not to provide a targeted attack platform for exploitation.

d. What security solutions are being utilised?

- Mail filtering
- Web Filtering
- Anti-Virus
- Firewall

e. What were the installation dates of the above network vendor(s)? (Month/Year)

- Mail Filtering 2002
- Web Filtering March 2017
- Anti-Virus February 2017
- Firewall 2013

f. When is your planned (or estimated) Network refresh date? (Month/Year)?

- 09/2018

g. What is your estimated budget for the Network refresh?

- Nil – procurement completed

h. When did you install your current Wi-Fi environment?

- April 2012

5. End User Devices:

a. How many desktops/laptops are deployed by the Council?

- 263

- b. How many mobile devices [Phones & tablets etc] are deployed by the council?
- 139
- c. What were the installation dates of the above desktop/laptops?
- 9 Jan-17
 - 1 Oct-16
 - 4 Aug-15
 - 1 Dec-14
 - 10 Mar-14
 - 4 Dec-13
 - 7 May-13
 - 122 Mar-13
 - 70 Feb-23
 - 8 Dec-12
- d. When is your planned (or estimated) desktop/laptop refresh date? (Month/Year)
- 09/2018
6. Backup, DR and BC:
- a. What device/system do you use for your daily backups (e.g tape or disk)
- Disk to Disk
- b. What backup software do you use?
- Veeam Backup and Replication
- c. How much data do you backup, in TB?
- 44TB
- d. Do you use a third party to provide a Business Continuity service (e.g. office workplace recovery or infrastructure ship-to-site solutions)?
- Yes
- e. Does your current recovery solution meet your stakeholder's expectations?
- Yes but this is currently being reviewed
- f. Do you already backup into the cloud?
- No
- g. Do you have a documented disaster recovery & business continuity plan in place?
- Yes but this is currently being reviewed
7. Number of Physical servers?
- 7
8. Number of virtualised servers? & Which Virtualisation platform do you use?

- Hyper-V
 - 74 Virtual Servers
9. Do you have a cloud strategy if so what is it?
- Yes and is based on business case per application
10. Do you use Azure or Amazon Web Services?
- No
11. Do you use or are you planning to use MS O365?
- Currently migrating to O365
12. Please also name all of the IT re-sellers that you work with and buy from, as well as the frameworks utilised.
- Civica
 - Softcat
 - Upgrade Options
 - Complete IT
13. Do you have a Software Asset Management Policy? If so what is it?
- No
14. Who is responsible for your Software Asset Management?
- Cliff Dean, ICT Manager, cliff_dean@n-kesteven.gov.uk , 01529 414155
15. How much did you pay in the last financial year for software licenses?
- Total for 17/18 = £266,161.80
16. If applicable, how many people are using Office 365?
- 4
17. Who are your top three software vendors by revenue?
- Civica, Northgate, Statmap
18. What are the contractual renewal dates for those three vendors?
- Civica - 1st April Annually
 - Northgate Revenues and Benefits - 31st December 2019
 - Statmap 1st April Annually
19. Have you been audited by those three vendors? If so the date of the audit.
- No
20. Do you currently measure software usage versus the number of licenses purchased?
- Yes

21. Do you use a software asset management and/or software inventory tool? If so which one(s)?

- Yes, LanSweeper

22. Are you actively moving any applications/infrastructure into a cloud environment? If so who is responsible for this?

- No

23. What is the total number of IT staff employed by the organization: Please list and provide contact details for the IT senior management team including CIO, IT Director and Infrastructure Architects if applicable.

- 4

24. Who is Head of IT? – Please provide contact details

- Cliff Dean, ICT Manager, cliff_dean@n-kesteven.gov.uk , 01529 414155

25. Who is Head of Procurement? – Please provide contact details

- Cliff Dean, ICT Manager, cliff_dean@n-kesteven.gov.uk , 01529 414155

26. Do you have a managed/shared service with any other councils?

Yes

27. Do you normally purchase equipment and services as a capital investment (Cap-Ex) or ongoing operational charges (Opex).

- Opex