Request:

1. In the past three years has your organisation:

a. Had any ransomware incidents? (An incident where an attacker attempted to, or successfully, encrypted a computing device within your organisation with the aim of extorting a payment or action in order to decrypt the device?) **None**
b. If yes, how many?
c. Had any data rendered permanently inaccessible by a ransomware incident (i.e. some data was not able to be restored from back up.) **No**
d. Had any data rendered permanently inaccessible by a systems or equipment failure (i.e. some data was not able to be restored from back up.) **No**
e. Paid a ransom due to a ransomware incident / to obtain a decryption key or tool? **No**
f. If yes was the decryption successful, with all files recovered?
g. Used a free decryption key or tool (e.g. from https://www.nomoreransom.org/)? **No**
h. If yes was the decryption successful, with all files recovered?
i. Had a formal policy on ransomware payment? **No**
j. If yes please provide, or link, to all versions relevant to the 3 year period.
k. Held meetings where policy on paying ransomware was discussed? **No**
l. Paid consultancy fees for malware, ransomware, or system intrusion investigation **No**
m. If yes at what cost in each year?
n. Used existing support contracts for malware, ransomware, or system intrusion investigation? **No**
o. Requested central government support for malware, ransomware, or system intrusion investigation? **No**
p. Paid for data recovery services? **No**
q. If yes at what cost in each year?
r. Used existing contracts for data recovery services? **No**
s. Replaced IT infrastructure such as servers that have been compromised by malware? **No**
t. If yes at what cost in each year?
u. Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware? **No**
v. If yes at what cost in each year?

w. Lost data due to portable electronic devices being mislaid, lost or destroyed? **No**

x. If yes how many incidents in each year?

2. Does your organisation use a cloud based office suite system such as Google Workspace (Formerly G Suite) or Microsoft's Office 365? **MS365**

a. If yes is this system's data independently backed up, separately from that platform's own tools? **Yes, we use MS365, but not independently backed up**

3. Is an offsite data back-up a system in place for the following? (Offsite backup is the replication of the data to a server which is separated geographically from the system's normal operating location site.)

a. Mobile devices such as phones and tablet computers **No**
b. Desktop and laptop computers **No**
c. Virtual desktops **These are backed up offsite via BaaS**
d. Servers on premise **Windows based servers are backed up offsite via BaaS**
e. Co-located or hosted servers **We have no co-located / hosted servers**
f. Cloud hosted servers **N/A at present**
g. Virtual machines **Windows based servers are backed up offsite via BaaS**
h. Data in SaaS applications **This is the responsibility of the supplier**
i. ERP / finance system **No**
j. We do not use any offsite back-up systems **N/A**

4. Are the services in question 3 backed up by a single system or are multiple systems used? **Windows based servers and data are backed up offsite via BaaS**

5. Do you have a cloud migration strategy? If so is there specific budget allocated to this? **Yes, there is no specific budget allocated to this**

6. How many Software as a Services (SaaS) applications are in place within your organisation? **There are 22 externally hosted applications**

a. How many have been adopted since January 2020? **None**