EAST CAMBRIDGESHIRE DISTRICT COUNCIL
THE GRANGE, NUTHOLT LANE,
ELY, CAMBRIDGESHIRE CB7 4EE
Telephone: Ely (01353) 665555
DX41001 ELY Fax: (01353) 665240
www.eastcambs.gov.uk

Further to your information request FOI/EIR 21/22-178 please find your question and our response below.

**Request:**

I am writing to you under the Freedom of Information Act 2000 to request the following information from East Cambridgeshire. Please can you answer the following questions:

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? )
        i. If yes, how many?
    b. Had any data rendered permanently inaccessible by a ransomware incident (i.e. some data was not able to be restored from back up.)
    c. 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.)
    d. Paid a ransom due to a ransomware incident / to obtain a decryption key or tool?
        i. If yes was the decryption successful, with all files recovered?
    e. Used a free decryption key or tool (e.g. from https://www.nomoreransom.org/)?
        i. If yes was the decryption successful, with all files recovered?
    f. Had a formal policy on ransomware payment?
        i. If yes please provide, or link, to all versions relevant to the 3 year period.
    g. Held meetings where policy on paying ransomware was discussed?
    h. Paid consultancy fees for malware, ransomware, or system intrusion investigation
        i. If yes at what cost in each year?
    i. Used existing support contracts for malware, ransomware, or system intrusion investigation?
    j. Requested central government support for malware, ransomware, or system intrusion investigation?
    k. Paid for data recovery services?
        i. If yes at what cost in each year?
    l. Used existing contracts for data recovery services?
    m. Replaced IT infrastructure such as servers that have been compromised by malware?
        i. If yes at what cost in each year?
    n. Replaced IT endpoints such as PCs, Laptops, Mobile devices that have been compromised by malware?
        i. If yes at what cost in each year?
    o. Lost data due to portable electronic devices being mislaid, lost or destroyed?
        i. 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?
    a. If yes is this system's data independently backed up, separately from that platform's own tools?

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
    b. Desktop and laptop computers

c. Virtual desktops
d. Servers on premise
e. Co-located or hosted servers
f. Cloud hosted servers
g. Virtual machines
h. Data in SaaS applications
i. ERP / finance system
j. We do not use any offsite back-up systems

4. Are the services in question 3 backed up by a single system or are multiple systems used?

5. Do you have a cloud migration strategy? If so is there specific budget allocated to this?

6. How many Software as a Services (SaaS) applications are in place within your organisation?
    a. How many have been adopted since January 2020?

**Response:**

In respect of those requests that where answered in full or partially and the total refused please take this as notice under FOIA, that we:
a) Consider the information as exempt from disclosure under the Act;
b) Claim exception under Sections of the Act:
**Exemption 31 – Law Enforcement**
c) State why the exemption applies:
**(1) Information which is not exempt information by virtue of section 31 is exempt information if its disclosure under this Act would, or would be likely to, prejudice - (a) the prevention or detection of crime, (b) the apprehension or prosecution of offenders.**
**As this exception is qualified, we are obliged to outline the harm in disclosure and explain why we consider that the public interest in maintaining the exception outweighs the public interest in disclosure:**
**While there may be public interest in knowing this information, the ICT Department considers that providing the requested information would, or would be likely to, substantially prejudice and present a significant risk to the security arrangements in place to protect the Council's network, as well as information and data held by our Council. This is confirmed the Information Commission's Office guidance on Exemption 31 of the Freedom of Information Act 2000, where it states 'The exemption covers information held by public authorities without any specific law enforcement responsibilities. It could also be used to withhold information that would make anyone, including the public authority itself, more vulnerable to crime by disclosing its own security procedures.' We believe the public interests in maintaining the security of our systems overrides the public interest in making details of Cyber Security incidents public and therefore neither confirm nor deny any ransomware incidents.**

This concludes your request FOI/EIR 21/22-178

If information has been refused please treat this as a Refusal Notice for the purposes of the Act.

If you disagree with our decision or are otherwise unhappy with how we have dealt with your request in the first instance you may approach foi@eastcambs.gov.uk and request a review. A request for review must be made in no more than 40 working days from the date of this email.

Should you remain dissatisfied with the outcome you have a right under s50 of the Freedom of Information Act to appeal against the decision by contacting the Information Commissioner, Wycliffe House, Water Lane, Wilmslow SK9 5AF.