Local Council Public Advisory Service

The Vision Centre
5 Eastern Way
Bury St Edmunds
Suffolk
IP32 7AB

www.lcpas.co.uk

General Data Protection Regulations

COMPLIANCE REPORT

Felixstowe Town Council

Back Ground:

The Government and the Information Commissioner announced the intention to incorporate the European General Data Protection Regulations within a new Data Protection Bill. This came into force on the same day as the General Data Protection Regulations on 25th May 2018.

The new regulations introduced enhanced protections for personal information held by a Local Authority, Business or Charity. The protection will now extend beyond files stored electronically to now include hard copy files.

The definition of personal data will be extended to include computer IP addresses and cookie files as these can trace an email or interaction back to the originating pc and identity of its user.

'IP ("eye-pea") is actually part of a longer abbreviation — TCP/IP. That stands for Transmission Control Protocol/Internet Protocol. (We'll call it IP for short.) IP stands for 'Internet Protocol.' A protocol is a guideline that must be followed in a set, specific way. Your computer has an IP address, your phone has an IP address. Even Coke machines have IP addresses.

What exactly is an "IP address"? Answer: IP address, or "internet protocol address", is a unique identifying number given to every single computer on the Internet. Any system that is connected to a network needs an IP address to communicate with other systems in the network. IP addressing is logical addressing, and can change.'

There are greater penalties for loss or damage to personal data and there is an expectation that Parish and Town Councils will have to consider encryption of data and emails and to also protect the Councils PCs from malware, viruses and ransomware all of which pose a threat to personal data on computers.

Hard copy files, which contain any personal data, will have to be protected from unauthorised access and damage.

The public will gain new rights around how their data is handled, stored and used. Parish and Town Councils will have to gain express consent to hold information and retain the consent forms on file as evidence.

All bodies that keep personal information will be required to produce privacy notices that include why and how data is collected, how long it will be kept and the public rights to be removed and how to amend and delete their records.

LCPAS recognised that the changes would have a significant impact on Parish and Town Councils and introduced a Data Protection Officer Service. As part of this service councils can opt to have a compliance visit. This is intended to provide some peace of mind.

Felixstowe Town Council invited LCPAS to undertake a compliance visit and produce a report on our findings.

Information Privacy

The ability of a person to control, edit, manage and delete information about themselves and to decide how and what extent such information is communicated to others.

Intrusion can come in the form of a collection of excessive personal information, disclosure of personal information without consent and misuse of such information.

Parish and Town Councils hold many forms of personal information including:

Correspondence including letters, emails, consultations, complaints
Contact databases including email address books and databases
Telephone call records
Planning Applications
Personnel including employee details, medical records, appraisals and salaries
Records related to recruitment, applications, CVs, letters, emails
Ex Councillor details and register of interests
Non-Councillors on Council Committees and working groups
Grant applications and correspondence
Electoral Rolls
Public reports on issues by email, letter and telephone
Fixed Penalty Notices
Allotment Tenancies and correspondence including invoices
Cemetery Records, Exclusive Right of Burial, correspondence, invoices
Hire Records for Halls and facilities
Sales information for Council run services including entertainment
Events, tickets or invitation lists

LCPAS has taken an overview of the hardcopy data that the council holds and in our report we make any recommendations that we feel may help the council to become compliant in the way they store Personal Information. We cannot be responsible for any files that were missed or not available or that have been added at a later date. During the IT security audit we check files and security arrangements we do not change any settings or open any documents. We make recommendations for your IT consultant to put in place enhanced security and if required additional software. LCPAS does not accept any liability for loss of data or functionality of computers after installing security software. All software should be obtained from an official and reputable source and installed following the instructions provided.

We are aware that our activities are disruptive, although we do strive to limit the impact on everyone concerned.

We would like to sincerely thank Felixstowe Town Council staff for their hospitality and assistance through the process.

Felixstowe Town Council

Main Office Area – **Low risk**

Felixstowe Town Council have taken excellent steps towards GDPR Compliance

The Councils main office is within the Town Hall complex which resides behind a reception area. There is no direct public access into the office. Both the main office and Town Clerks office have locked doors when not in use. The building is locked and alarmed.

All HR related documents are kept in the Town Clerks office and locked away.

GDPR General Privacy notice in place and on website

Data Protection Policy and Retention of Documents Policy are in place as is the Staff notice and employee privacy notice.

The Town Council intends to move Councillors over to a Council email address following the election in May 19.

The Public may hire the facilities for events and weddings but they have no access to the Town Council Offices.

All personal information is stored in lockable cabinets
Documents containing personal information including HR have all been sorted through and locked away.

We found the security measures in place to be excellent. This includes office security, file security and IT.

Risks and Remedies

The risk of data being removed or lost is low for this area. Overall the security is good and the filing cabinets and draws holding all the Town Council Information is always locked.

However, taking the steps below may reduce the risk even further.

In making our recommendations, we have taken into account space and options available.

We made just a couple of minor recommendations.

That a privacy statement be displayed next to the signing in book in reception. That the anti virus software be checked to ensure all machines are up to date.

We do not recommend that any folders that hold any hard copy personal data should not leave the premises. This reduces the risk of loss or damage to data but we also realise that staff may need to if they are working from home on anything. We therefore recommend a booking out policy for documents that ensure that any documents are returned intact by a specified time as stated above.

The Council should consider having a policy for achieving or disposing of old records in accordance with retention of document policy. This gives the amount of time each type of document has to be kept for.

****

Security of Electronic Data

We undertook a spot check of security on the Council's IT provisions to measure the risks to the infrastructure and data held electronically.

Risks and Remedies

Overall the security on the PC we spot checked was excellent once the issues highlighted below have been implemented.

We found that the network antivus had been disabled as had Windows Defender which left the machine and network vulnerable. We notified staff of the issue and this was immediately addressed with the Councils IT company.

Panda Endpoint security system provides an antivirus, firewall and malware protection.
The Council could also enable Windows Defender as this can run along side Panda to give extra protection.

We checked two other PCs and found them to be in good order with the antivirus software and firewall functioning

The PC had access to the Councils shared network drives including the staff folder. We recommend using Folderlock which installs a lockable folder. This folder can contain confidential information, HR, sensitive data and be protected by a single password.

The Council uses Bitlocker to encrypt PC drives and Office 365 to encrypt emails.

Remote desktop is enabled, and this is usually so that an IT company can access the PC to remedy issues. We note that the user would have to give consent for anyone to remotely access the machines.

The PCs are of a very good specification and we found no physical faults.

The Council could also consider online backup rather than by an external drive.
This is a safer and more reliable method of back up as it cannot be damaged, dropped or lost.

We did not access the internet gateway (router) but they should have several security features enabled.

1. WPA2 Encryption to prevent unauthorised access to the internet
2. Built-in Firewall This can be a great tool for allowing or denying traffic originating from the Internet, preventing it from reaching your computer. You can also use it to control what traffic leaves your network as well.
3. VPN at the router by setting it up at the router level and all network traffic going in and out of your network will be protected by encryption.

Emails are a weakness as they can be exchanged with many recipients and also forwarded on to other parties outside of the Council. We recommend that everyone (including Councillors) consider whether the names and details of the person concerned are required.

We also recommend that the Councillors consider instalingl encryption software within email clients. There is an excellent free plug in called Virtru. Microsoft recommends it on its security website linked to its Trust Centre settings. Virtru is quick to install and allows the user to decide whether an email and its attachment require encrypting. To encrypt you would click on the encrypt button installed within your email client, and it is securely sent and encrypted.

Please see link below:

https://www.virtru.com/

Folderlock can protect multiple files with one password

https://www.microsoft.com/en-gb/store/p/folder-lock/9nblggh187z7

Axcrypt can encrypt and protect files, folders or complete hard drives. There is a free version but we would recommend considering the fully featured version costing £24 per year per license. There is also free encryption software available called Veracrypt which is based on the very successful TrueCrypt software. Veracrypt is provided free on an open source license.

Please see link below:

https://www.axcrypt.net/pricing/
https://www.veracrypt.fr/en/Home.html

Backup:

We recommend that the Council consider using an online back-up provider rather than an external drive. The programs are easy to use, and they can in some cases act like a server for sharing files and folders between staff. They come with high security and reliability. However, they are dependent on an Internet connection. There are free versions and purchase versions. We recommend the software below, you are free to explore other providers.

Please see the link below:

Dropbox £60 per month, unlimited space and up to 5 users
https://www.dropbox.com/business/landing-t61fl?&_tk=sem_b_goog&_camp=sem-b-goog-uk-eng-top-exact&_kw=drop%20box%7Ce&_ad=49517599542%7C1t1%7Cc&gclid=EAIaIQobChMIibr2sZ-L1gIVDpPtCh23zAO5EAAYASAAEgL_E_D_BwE

A Drive starting at £70 per year, 200gb to unlimited, multiple user accounts
http://www.adrive.com/plans

We also recommend that the Council insures the equipment and users from the liability of any action taken against them for any loss or damage to data. We also recommend that the Council indemnify by insurance Councillors and Staff against loss or damage to data and other linked activities.

We recommend that all Councillors are trained so that they all fully understand the implications of the new data protection legislation.

The cost of implementing changes will depend on the options the Council wishes to explore. We have recommended a number of free and, to purchase software options. The Council should consider the merits of each one before deciding which route to take. There are also other packages on the market that the Council may wish to consider.

Always back up the PCs before installing new software and scan any downloads for viruses. Also, only download software from the official site or a reputable source.

Jayne Cole
Chief Executive Officer
Local Council Public Advisory Service