Local Council Public Advisory Service

6 Aragon Court
Clare
Suffolk
CO10 8FA
Tel: 01787 829576

www.lcpas.co.uk

GDPR Compliance Visit

Redlodge ParishCouncil

Privacy Impact Assessment

Back Ground:

The Government and the Information Commissioner have recently announced the intention to incorporate the European General Data Protection Regulations within a new Data Protection Bill. Once the Bill attains Royal Assent it is intended to come into force on the same day as the General Data Protection Regulations 25 May 2018.

The new regulations introduce 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.

... But 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.

The Information Commissioners Office issued advice that all affected Authorities, Businesses and Charities should start to make plans for compliance a year in advance. Ensuring that they would be compliant in time for the new Act to come into force.

It also advised that it would be beneficial for those affected to undertake a Personal Impact Assessment to investigate how the new law would affect them and what could be put in place to mitigate the risk. The ICO also advised that the new legislation was likely to have significant resource implications. This was both in manpower and financially by putting measures in place to protect IT infrastructure, electronic and hard copy files.

LCPAS recognised that the changes would have a significant impact on Parish and Town Councils and introduced training on the changes and also provide Data Protection Officer Service. As part of the service we offered a compliance visit to assist Councils and to provide peace of mind.

Redlodge Parish Council invited LCPAS to undertake a compliance visit

Information Privacy

GDPR gives 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 makes every effort to audit as many folders containing data as possible. 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 Wendy for her hospitality and assistance through the process.

Redlodge Parish Council

The Town Clerks office is located in a building and forms part of a community facility. The main door is accessed off the side of the building. The office is secure from public access.

Hardcopy personal information files are kept on open shelves and we recommend moving the stationary onto the shelves and documents with personal information into the lockable stationary cupboard.

The Council has started the process towards compliance. This will need to include a Data Protection Audit to locate personal information within hard copy files and deciding whether to dispose, achieve or move into secure storage in line with the retention of documents policy.

A lockable key box for would also be of benefit. This would keep all keys safe in one secure location with one key.

The Council has CCTV and will require a policy and privacy statement to cover its use.

Data Protection Policies and Privacy Notices are being produced for Council approval

Information Flow:

The information has been acquired over the years and can be accessed by members of staff.

Recommendations:

Risks and Remedies

The risk of data being removed or lost are medium for this area. This is because the office door is lockable. However, Personal Information needs to be moved into a lockable cabinet. A cleaner also has access to this area and Groundmen.

The risk could be further reduced by following the recommendations below:

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

The Council could consider a clear desk policy and that working papers, note books with unstructured data are placed in a desk draw when not in use.

****

Store Cupboard (Archive)

The storeroom is in the corridor off the Clerks office and is locked.

The locked store cupboard holds Town Councils archive documents and files. The Council has been going through the process of sorting through these files with the intention of either archiving, retaining or shredding them.

Recommendations

We do not recommend that Council documents leave the premises 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.

We recommend that the Parish Council consult with Suffolk Records Office regarding what historical documents could be deposited and that any documents no longer require are disposed of in line with the Document Retention Policy.

aterial Cost of Securing Hard Copy Data

Costs:

There will be indicative costs implementing the changes, these have been estimated as.

- Staff time in re-organising files and folders including shredding and archiving.
- This could be several hours work estimated at £600
- The cost of replacing the filing cabinets locks (if applicable) at £5.97 per unit
- https://www.fastkeys.co.uk/multi/product/7B63E0F1AFA4D62F80257F6E006070E8
- The cost of a booking in and out files and folders book x 2 = £6.00
- Secure lockable boxes x 2 £20

****

Security of Electronic Data

We undertook a security audit of the Councils IT provisions to measure the risks to the infrastructure and data held electronically.

Computers are of a good specification

The Council has three machines that are connected to the internet and a shared drive.

The Operating systems on the machines Windows 7 will require updating to Windows 10 as 7 has a limited lifetime of security support. – Windows 7 is fully supported until Jan 2020 so there shouldn't be any need to do anything about this until this time

Commented [MM1]:

Antivirus and firewall software have been installed on both machines and Windows defender is enabled. Windows security updates are enabled and up to date. The Smart Norton Firewall and Windows Firewall on the finance machine are not enabled. This needs to be remedied and Norton and Windows enabled. This is the case because remote access was required outside the ce to the finance machine and data – a decision may need to be made about whether this is required or whether you are comfortable with the risk.

Commented [MM2]:

The Clerks machine back up to Elephant Drive is not enables and this will require attention. We do probably need to check this out as it should be enabled.

Commented [MM3]:

The network is set to private and the machines are not visible to other networks.

Any sensitive files and documents including personal information, HR and confidential matters should be contained within a password protected or lockable folder. We recommend that the Council consider using Folderlock. – You shouldn't need any additional software here as we can change the permissions on the server- if you tell us what things need to be secured anyway then we can sort this.

Commented [MM4]:

We also recommend that the machines are checked from time to time to ensure all security updates and antivirus updates are being installed.

If the IT provision changes, added to or machines replaced a risk assessment should be undertaken and steps to put all security measures in place before using it.

We did not access the internet gateway (router) but they should have a number of 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. – These measures are all in place

Commented [MM5]:

The Council does not encrypt its files, folders, drives or emails. We recommend that the Council secures electronic data in this way. If information is lost or damaged it will be very difficult to access. We have identified reliable software below that can offer secure encryption for a modest cost. It's probably sensible to deal with this when Windows 10 is installed. Encryption software Bitlocker comes with Windows 10 and should be able to be used in this scenario.

Commented [MM6]:

Please see the link below:

http://www.clamwin.com/content/view/18/46/

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. Instead of just forwarding emails it will be safer to cut and paste the content into a new email. This will not pass on any information held in the original emails header, including IP address.

We also recommend that the Council install encryption software within email clients. There is an excellent free plug in called Virtu. Microsoft recommends it on its security website linked to its Trust Centre settings. Virtu 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. I'm personally not convinced this is really required. There is an argument for it but for now I'd probably recommend not to install.

Commented [MM7]:

Please see link below:

https://www.virtru.com/

During the examination of the laptops we did discover that some sensitive folders were accessible to all staff. We recommend that the Council considers installing Folder Lock. This is an excellent piece of software that is intuitive to use. It simply locks folders with a password set by the user. To open the folder the user enters the password and the folder opens. Folder Lock is available to purchase for £2.29 per machine for the fully featured version. You shouldn't need any additional software here as we can change the permissions on the server- if you tell us what things need to be secured anyway then we can sort this.

Commented [MM8]:

Please see link below:

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

Bitlocker on Windows 10 pro would fulfill this function should the Council wish to upgrade the PCs.

Please see link below:

Bitlocker is a recognised and trusted encryption programe. It is available if the PCs are upgraded to Windows 10 Pro.

https://computerbuilders.co.uk/windows-10-pro-product-key?gclid=EAIaIQobChMI0Jfl5ZiL1gIVyLftCh2i4wA2EAYYBCABEgJRPfD_BwE

An alternative route would be to install stand alone file encryption software. Axcryp 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. Vercrypt 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. 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. You already use Elephant Drive – which is a cloud provider - so no need to do anything here.

Commented [MM9]:

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