MUCH HADHAM PARISH COUNCIL - GDPR RISK ASSESSMENT MAY 2018

Area of risk	Risk Identified	Risk Level H/M/L	Management of Risk	Action taken/completed
All personal data	Personal data falls into hands of a third party	H	Identify what personal data your council holds. Examples include the Electoral Roll, Job applications, tenancy agreements), why it holds it and for how long, who it shares with (see separate Assessment of Personal Data held by councils)	Full identification of what personal data held is outstanding. Initial Assessment of Personal Data has been completed. Personal data held by Cllrs unknown.
		H	Identify how you store personal data. Examples include paper files, databases, electronic files, laptops and portable devices such as memory sticks or portable hard drives.	Clerk stores personal data securely in home. Paper in files which are only accessed by Clerk; electronic on devices with password protection. Cllrs – currently unknown.
	Publishing of personal data in the minutes and other council documents	L	Avoid including any personal information in the minutes or other council documents which are in the public domain. Instead of naming a person, say 'a resident/member of the public unless necessary.	Excluding Cllrs and the Clerk, all documentation in the public domain excludes personal information.
Sharing of data	Personal data falls into hands of a third party	M	Does your council share personal data with any other organisations, for example other local authorities? If yes, you may need to set up a written agreement with the organisation to ensure that they protect the data once passed to them	Potential sharing area relates to interments and memorials. Being discussed with funeral directors and MHPC form to be changed. Information is shared with EHC & HCC Cllrs – what's the status of this?
Hard copy data	Hard copy data falls into hands of a third party	M	Decide how much of the personal data held is necessary. Destroy personal data which is no longer needed in line with the Retention of Documents policy	Clerk retains in accordance with Retention Policy – revised policy for approval at 1 May 2018 meeting. Cllrs – unknown
		L	Ensure that sensitive personal data is stored securely in a locked room or cabinet when not in use	No such data is held and it is envisaged that it never will be.
		H	If using a shared office operate a clear desk policy when not at desk at the end of the day Cash handling is avoided, but where necessary appropriate controls are in place	Clerk's office not shared (L) but position relating to Cllrs currently unknown.
Electronic data	Theft or loss of a laptop, memory stick or hard drive containing personal data	H	Ensure that all devices are password protected	Clerk's devices are password protected (L) but position relating to Cllrs currently unknown.
		M	Make all councillors aware of the risk of theft or loss of devices and the need to take sensible measures to protect them from loss or theft	Awareness raised at PC meetings in December 2017 & April 2018. Cllrs to complete, sign and return awareness checklist.
		H	Carry out regular back-ups of council data	Clerk is low risk but position relating to Cllrs currently unknown.

H = High Risk | M = Medium Risk | L=Low Risk

Area of risk	Risk Identified	Risk Level H/M/L	Management of Risk	Action taken/completed
		L	Ensure safe disposal of IT equipment and printers at the end of their life	Currently, no IT equipment owned by the PC
		L	Ensure all new IT equipment has all security measures installed before use	See above. Laptop to be purchased and will have Microsoft package + password protection + McAfee antivirus protection.
Email security	Unauthorised access to council emails	H	Ensure that email accounts are password protected and that the passwords are not shared or displayed publicly.	Clerk's email account password protected and not shared (L) but position relating to Cllrs currently unknown.
		H	Set up separate parish council email addresses for employees and councillors (recommended)	Clerk has dedicated PC email address (L) but position relating to Cllrs currently unknown.
		H	Use blind copy (bcc) to send group emails to people outside the council	Clerk does not send group emails (L). Position relating to Cllrs currently unknown.
		H	Use encryption for emails that contain personal information	This is not currently done. Protocol to be developed and agreed.
		H	Use cut and paste into a new email to remove the IP address from the header	This is not currently done. Protocol to be developed and agreed.
		H	Do not forward on emails from members of the public. If necessary, copy and paste information into a new email with personal information removed.	This is not currently done. Protocol to be developed and agreed.
		H	Delete emails from members of public when query has been dealt with and there is no need to keep it	Clerk is in process of deleting emails in accordance with Document Retention Policy – being updated(M). Position relating to Cllrs currently unknown.
General internet security	Unauthorised access to council computers and files	H	Ensure that all computers (including councillors) are password protected and that the passwords are not shared or displayed publicly	Clerk laptop is password protected and not shared (L) but position relating to Cllrs currently unknown.
		H	Ensure that all computers (including councillors) have up-to-date anti-virus software, firewalls and file encryption is installed.	Clerk's laptop is updated and secured (L) but position relating to Cllrs currently unknown.
		H	Ensure that the operating system on all computers is up-to-date and that updates are installed regularly	Clerk's laptop is updated and secured (L) but position relating to Cllrs currently unknown.
		L	Password protect personal and sensitive information folders and databases. Ensure that shared drives do not provide unauthorised access to HR and other records containing personal information	No sensitive personal data collected or held.

Area of risk	Risk Identified	Risk Level H/M/L	Management of Risk	Action taken/completed
Website security	Personal information or photographs of individuals published on the website	M	Ensure that you have the written consent of the individual including parental consent if the subject is 17 or under) Ensure you have a Vetting and Barring Policy	No data subject under 17 on the website. Not 100% sure that there is no personal data on the website. No Vetting and Barring Policy – but what is this and is it required? If relates to children, then not applicable.
Disposal of computers and printers	Data falls into the hands of a third party	H	Wipe the hard drives from computers, laptops and printers or destroy them before disposing of the device	But is this not common sense regardless of connection with PC? Sledgehammer very effective.
Financial Risks	Financial loss following a data breach as a result of prosecution or fines	L	Ensure that the council has liability cover which specifically covers prosecutions resulting from a data breach and put aside sufficient funds (up to 4% of income) should the council be fined for a data breach	Whilst reference is to out of date data protection legislation, PC has cover in place for a data breach.
	Budget for GDPR and Data Protection	L	Ensure the Council has sufficient funds to meet the requirements of the new regulations both for equipment and data security and add to budget headings for the future	Budget for 2018/19 includes sufficient funding to ensure compliance with GDPR will be achieved
General risks	Loss of third party data due to lack of understanding of the risks/need to protect it	H	Ensure that all staff and councillors have received adequate training and are aware of the risks	Clerk has had training (L) but position relating to Cllrs currently unknown. Cllr training on the 24th April 2018 had to be cancelled due to low numbers. Number of Cllrs being trained through workplaces – need to get evidence of this, including content.
	Filming and recording at meetings	L	If a meeting is closed to discuss confidential information (for example salaries, or disciplinary matters), ensure that no phones or recording devices have been left in a room by a member of the public	Only confidential meeting is the Staffing Committee which meets with press and public excluded.

GDPR risk assessment approved at the 1 May 2018 meeting.