# GDPR Risk Assessment

**Name of Council: Swettenham Parish Council** **Date: 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 | L | Identify what personal data your council holds. Examples include the Electoral Roll, Job applications), why it holds it and for how long, who it shares with | Assessment prepared |
| | | M | 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. | Laptop and USB memory sticks |
| | 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. | State 'resident' or 'parishioner' |
| **Sharing of data** | Personal data falls into hands of a third party | L | 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 | No personal data sharing |
| **Hard copy data** | Hard copy data falls into hands of a third party | L | 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 working through this |
| | | L | Ensure that sensitive personal data is stored securely in a locked room or cabinet when not in use | No shared office. Clerk is only employee and works from home |
| **Electronic data** | Theft or loss of a laptop, memory stick or hard drive containing personal data | M | Ensure that all devices are password protected | Complete |
| | | 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 | Councillors made aware at the Council Meeting on 21st May 2018 |
| | | M | Carry out regular back-ups of council data | This is done on a regular basis |
| | | M | Ensure safe disposal of IT equipment and printers at the end of their life | To be done when necessary |
| | | M | Ensure all new IT equipment has all security measures installed before use | Complete |
| **Email security** | Unauthorised access to council emails | M | Ensure that email accounts are password protected and that the passwords are not shared or displayed publicly. | Complete |
| | | M | Set up separate parish council email addresses for employees and councillors (recommended) | Clerk has separate Council email address to personal email |
| | | M | Use blind copy (bcc) to send group emails to people outside the council | Daily |
| | | M | Use encryption for emails that contain personal information | Daily |
| | | M | Use cut and paste into a new email to remove the IP address from the header | Daily |
| | | M | Do not forward on emails from members of the public. If necessary copy and paste information into a new email with personal information removed. | Daily |
| | | M | Delete emails from members of public when query has been dealt with and there is no need to keep it | Daily |

| | | | | |
|---|---|---|---|---|
| **General internet security** | Unauthorised access to council computers and files | M | Ensure that all computers (including councillors) are password protected and that the passwords are not shared or displayed publically | Laptop is in clerk's home |
| | | M | Ensure that all computers (including councillors) have up-to-date anti-virus software, firewalls and file encryption is installed. | Clerk – Complete<br>Councillors – to action |
| | | M | Ensure that the operating system on all computers is up-to-date and that updates are installed regularly | Clerk - Complete<br>Councillors – to action |
| | | M | Password protect personal and sensitive information folders and databases. | No shared drives |
| **Website security** | Personal information or photographs of individuals published on the website | L | Ensure that you have the written consent of the individual including parental consent if the subject is 17 or under)<br>Ensure you have a Vetting and Barring Policy | No personal photographs on the website |
| **Disposal of computers and printers** | Data falls into the hands of a third party | M | Wipe the hard drives from computers, laptops and printers or destroy them before disposing of the device | To be done when necessary |
| **Financial Risks** | Financial loss following a data breach as a result of prosecution or fines | M | 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 | Covered under Council's Insurance Policy |
| | Budget for GDPR and Data Protection | M | 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 | To be added to Council budget |
| **General risks** | Loss of third party data due to lack of understanding of the risks/need to protect it | M | Ensure that all staff and councillors are aware of the risks | Councillors made aware at the Council Meeting on 21st May 2018 |
| | Filming and recording at meetings | M | 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 | To action when necessary |