ST MEWAN PARISH COUNCIL

ANNUAL DATA PROTECTION REPORT

ST MEWAN PARISH COUNCIL is the data controller for all attributable data gathered in the name of the authority for the conduct of its statutory functions and duties.

The internal audit of data management has been undertaken as part of its Risk Management Strategy and to demonstrate its commitment to the General Data Protection Regulations 2018.

NOTE :

RED – high risk identified and immediate action required

AMBER – actions identified partially implement or planned

GREEN – successfully implemented

1. **The Council has established an appropriate data protection policy.**

   You should put in place a standalone policy statement or a general staff policy on data protection. The policy should:

   - set out The Council's approach to data protection together with responsibilities for implementing the policy and monitoring compliance;
   - be approved by management, published and communicated to all staff; and
   - be reviewed and updated at planned intervals or when required to ensure it remains relevant.

   ICO GUIDANCE

   - Get safe online website

   Policy examples and templates are widely available online.

   STATUS: GREEN

RECOMMENDATIONS FOR ACTION :

2. The Council has made privacy notices readily available to individuals.

To ensure the processing is fair you must be transparent about how you intend to use the data in compliance with principles one and two of the DPA. You should:

- include privacy notices on your website and any forms that you use to collect data; and
- give clear explanations on privacy notices detailing the reasons for using the data, including any disclosures.

If you want to use personal data for a reason that was not covered in your privacy notice you should consider obtaining prior consent to ensure the new use is fair.

ICO GUIDANCE

- Collecting information about your customers, ICO
- Privacy notices code of practice, ICO
- Processing personal data fairly and lawfully, ICO Guide to data protection

STATUS: GREEN

RECOMMENDATIONS FOR ACTION :

3. The Council has established processes to ensure personal data is of sufficient quality to make decisions about individuals.

The third principle of the DPA requires that personal data is adequate, relevant and not excessive for your purposes. You should:

- avoid collecting data without a legitimate business reason and collect only the minimum required to meet the purposes specified in your privacy notice;
- document rules for creating and keeping records, including emails; and
- ensure that you record only factual information and, where you identify any inaccurate data, make sure you update the records accordingly.

ICO GUIDANCE

- The amount of personal data you may hold, ICO Guide to data protection
- Keeping personal data accurate and up to date, ICO Guide to data protection

STATUS: AMBER

RECOMMENDATIONS FOR ACTION: To review recommended asset and audit documents

4. The Council has established a process to routinely dispose of personal data that is no longer required in line with agreed timescales.

The fifth principle of the DPA requires that personal data should not be kept for longer than necessary. You should:

- identify and record what types of records or data sets you hold (an information asset register);
- implement processes to discard, delete or anonymise personal data as soon as it becomes surplus to requirements;
- introduce a written retention policy to remind you when to dispose of various categories of data, and help you plan for its secure disposal; and
- have a disposal schedule and destruction log to ensure that you are able to manage the destruction process effectively.

ICO GUIDANCE

- Retaining personal data, ICO Guide to data protection

STATUS : GREEN

RECOMMENDATIONS FOR ACTION :

5. The Council has established an information security policy supported by appropriate security measures.

The seventh principle of the DPA requires that personal data is protected by appropriate security measures. Before you can decide what level of security is right for The Council you will need to assess the risks to the personal data you hold and choose the security measures that are appropriate to your needs. You should:

- develop, implement and communicate an information security policy within your organisation;
- ensure the policy covers key information security topics such as access controls, physical security, network security, email and

internet use, storage and maintenance and security breach / incident management;
- implement periodic checks for compliance to policy to give assurances that security controls are operational and effective; and
- deliver regular staff training on all areas within the information security policy.

ICO GUIDANCE

- Information security, ICO Guide to data protection
- Staff policies, Get safe online website

STATUS: GREEN

6. The Council ensures an adequate level of protection for any personal data processed by others on your behalf or transferred outside the European Economic Area.

If you outsource the processing of personal data you may still remain responsible for the data under the DPA and therefore you should:

- choose an organisation that provides sufficient guarantees about how it will protect the data;
- ensure written and enforceable contracts are in place setting out information security conditions;
- consider whether outsourcing involves the transfer of data overseas (which could include hosted services or cloud computing solutions); and
- ensure the recipient will provide adequate protection.

ICO GUIDANCE

- Outsourcing: a guide for SMEs, ICO
- Information security, ICO Guide to data protection
- Sending personal data outside the European Economic Area, ICO Guide to data protection
- Data controllers and data processors: what the difference is and what the governance implications are, ICO

STATUS: GREEN

RECOMMENDATIONS FOR ACTION:

7. The Council has established processes to ensure new projects or initiatives are privacy-proofed at the planning stage.

A 'privacy by design' approach can help your organisation to reduce risks and avoid costly changes at a later date. You should:

- build in privacy considerations at the start of projects or initiatives that involve the processing of personal data;
- undertake privacy impact assessments (PIA) during the development, testing and delivery stages of any project; and
- develop and implement supporting PIA guidelines for staff.

ICO GUIDANCE

- Privacy impact assessment code of practice, ICO

STATUS: GREEN

RECOMMENDATIONS FOR ACTION:

8. The Council provides data protection awareness training for all staff.

Where measures have only been partially implemented, please select the appropriate actions from the detail below:

You should brief all staff handling personal data on their data protection responsibilities as follows:

- induction training - provide awareness training on or shortly after appointment;
- communication and updates to all staff at regular intervals or when required (for example, intranet articles, circulars, team briefings and posters); and
- specialist training for staff with specific duties, such as marketing, information security and database management.

ICO GUIDANCE

- Think privacy toolkit, ICO
- Training checklist for small to medium sized organisations, ICO

STATUS : GREEN

RECOMMENDATIONS FOR ACTION:

9. The Council has nominated a data protection lead.

YES - Cllr Holman

10. The Council has registered with the Information Commissioner's Office.

YES

11. The Council has established a process to recognise and respond to individuals' requests to access their personal data.

YES

Signed : *Wendy Yelland* on behalf of the Council Date : 8th May 2019

Role : Clerk and Responsible Financial Officer

Minute No: AC28/19

Review at Finance Meeting for ratification at Annual Meeting 2020