HOLME VALLEY PARISH COUNCIL

GENERAL DATA PROTECTION REGULATION (GDPR) CHECKLIST

The General Data Protection Regulation (GDPR) came into force on 25 May 2018. It replaces the existing law on data protection (Data Protection Act 1998) and gives individuals more rights and protection in how their personal data is used. Local (Parish/Town) Councils and charities must comply with its requirements, just like any other organisation that processes personal data.

Holme Valley Parish Council processes personal data as a 'data controller'. To do so, it must:

1. **Appoint a Data Protection Officer (DPO)**
    a. The Clerk will be the data Protection Officer

2. **Carry out a Data Audit**
    a. The Council must review its data processing.
    b. A template has been provided by NALC/YLCA .

3. **Issue Privacy Notices**
    a. The Council must produce a Privacy Notice, which is a policy setting out how personal data is processed and stored, the legal justification for doing so, and a person's rights regarding any personal data held by the Council.
    b. The Privacy Notice must be approved and adopted by full Council, and issued to anyone on whom the Council holds personal data, e.g. the Council's employees and maintenance contractor.
    c. The Privacy Notice should be published online, on the Council's website, for people to access.
    d. The Privacy Notice should be reviewed annually, e.g. at the last Finance & Management Committee meeting of a civic year, so that it can be re-approved and re-adopted at the Annual Council Meeting.

4. **Get Consent**
    a. It is likely that the Council will need to get additional consent from people where consent has been assumed previously or the evidence of consent is no longer available.

5. **Ensure GDPR Procedures are up to date**
    a. Data subjects (those people about whom the Council holds personal data) have the right to see what data is being stored about them, to make corrections where there are any errors, or to ask for their data to be deleted.
    b. The Council needs to have processes in place to meet such requests.

6. **Manage what to do in the case of a breach**
    a. The Council needs to develop a set of breach management procedures to ensure that it knows what to do in the event of a breach.

b. Data breaches must be reported (where this is required) to the Information Commissioner's Office **within 72 hours** of the breach.

Under the old Data Protection legislation, the maximum fine for a data breach was £500,000 in the UK, but under GDPR there will be a huge increase in fines, to £17m or 4% of annual turnover) which will place significant additional risk on the Council.

The GDPR will allow users to claim damages, e.g. where there has been a data breach or where processing of data is unlawful, so the Council may wish to seek advice from its insurer on whether additional cover is available, to cover for such an eventuality.

Additional costs may also be incurred, e.g. a GDPR breach could require the Council to spend substantial time, money and effort to respond to requests for access to personal data, enforcement notices and minimising any negative publicity.

The principle of accountability puts the compliance burden on the Council, requiring it to produce and maintain documents that demonstrate what actions have been taken to achieve compliance.

Liz Bennett
Clerk to the Council
July 2020