BRIEFING
DATA PROTECTION LAW

1. LEGISLATIVE FRAMEWORK

The key legislation is set out in the Data Protection Act (2018) which replaces and repeals the Data Protection Act (1998). Implementation of the General Data Protection Regulation (2018) is the main feature of the Data Protection Act (2018). The UK Government has made is clear that after Brexit the UK will continue to adopt a similar standard for data protection as set out in the General Data Protection Regulation.

The General Data Protection Regulation took effect from 25 May 2018. It gives individuals more rights and protection regarding how their personal data is used by organisations, including local authorities such as parish and town councils. The Regulation places a much greater emphasis on transparency, openness and the documents that are needed to show a parish council is complying with the legislation. The Regulation also imposes new burdens on parish councils including new reporting requirements and increased fines and penalties.

The Information Commissioner's Office is still the regulator in charge of data protection and privacy issues. Its role includes monitoring, enforcement, awareness, dealing with complaints and investigations. For example, the Office has the power to audit organisations that will need to be able to demonstrate and evidence compliance with the legislative requirements. The Office has the powers to issue warnings, reprimands and orders, as well as to issue penalties and fines that are "effective, proportionate and dissuasive".

2. DEFINITIONS

Data controller: This is the person or organisation who determines the how and the what of data processing. The data controller is Chawleigh Parish Council.

Data processor: This is the person or firm, e.g. a payroll management firm, that processes the data on behalf of the data controller. The data processor is usually the Clerk.

Data subject: This is the individual about whom personal data is processed.

Personal data: This is the information about a living individual who can be identified directly or indirectly using other information.

Sensitive personal data: This type of data is also called special categories of personal data under the General Data Protection Regulation. It includes information on racial or ethnic origin, political opinions, religious beliefs, Trade Union membership, physical or health conditions and data concerning an individual's sex life or sexual orientation. It also now includes both biometric data and genetic data for the purpose of uniquely identifying an individual.

Processing: This is anything done with or to personal data, e.g. obtaining, recording, storing, updating and sharing.

3. DATA PROTECTION PRINCIPLES

The Data Protection Act (2018) has six underlying principles that are mirrored in the General Data Protection Regulation (2018). Personal information should be:

1. Used lawfully, fairly and in a transparent way;
2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes;
3. Relevant to the purposes we have told you about and limited only to those purposes;
4. Accurate and kept up to date;
5. Kept only as long as necessary for the purposes we have told you about; and

6. Kept and destroyed securely including ensuring that appropriate technical and security measures are in place to protect your personal data to protect personal data from loss, misuse, unauthorised access and disclosure.

The General Data Protection Regulation has an additional principle of "Accountability" that places a much greater emphasis on transparency and openness. The compliance burden has been put on parish councils, requiring them to produce and maintain documents that demonstrate what actions have been taken to achieve compliance with the legislation and the six principles.

4. PROCESSING PERSONAL DATA

4.1 Personal data

Personal data is the information about a living individual who can be identified directly or indirectly using other information. There are six lawful bases for processing personal data. For most parish councils, a number of different lawful bases will apply at the same time. A parish council holds and processes personal data mainly for the following purposes:

- **Compliance with legal obligation**: The processing is necessary for the parish council to comply with the law (not including contractual obligations), e.g. employees' National Insurance numbers for tax purposes.
- **Contractual necessity**: The processing is necessary for a contract the parish council has with the individual, or because they have asked for the parish council to take specific steps before entering into a contract.
- **Consent**: The individual has given clear consent for their personal data to be processed for a specific purpose, e.g. parishioner contact list for circulating copies of the minutes. Consent is a positive, active, unambiguous confirmation that a data subject has agreed to have their data processed for a particular purpose. Consent must be easy to withdraw and must be freely given on an opt-in basis rather than opt-out.
- **Public interest**: The processing is necessary for the parish council to perform a task in the public interest or for the parish council's official functions and the task or function has a clear basis in law.

The other two lawful bases comprise:

- **Legitimate interest**: The processing is necessary for an organisation's legitimate interests or the legitimate in interests of a third party unless there is good reason to protect the individual's personal data which overrides those legitimate interests (This cannot apply as the parish council is a public authority processing data to perform its official tasks).
- **Vital interests**: The processing is necessary to protect someone's life, e.g. in a life or death situation it is permissible to use a person's medical or emergency contact information without their consent.

4.2 Sensitive personal data

This type of data is also called special categories of personal data under the General Data Protection Regulation (2018). It includes information on racial or ethnic origin, political opinions, religious beliefs, Trade Union membership, physical or health conditions and data concerning an individual's sex life or sexual orientation. It also now includes both biometric data and genetic data for the purpose of uniquely identifying an individual.

The data controller, i.e. the parish council, has to establish a lawful basis for processing any sensitive personal data (see paragraph 4.1 above). In addition, the data controller must establish that at least one criterion of a further list of criteria applies. In a parish council context, the criteria listed below represent the most relevant lawful bases for processing sensitive personal data:

- Explicit consent from the data subject has been obtained (which can be withdrawn);
- Employment Law (for staff); and

- Reasons of substantial public interest while performing the public authority's role of the parish council and where it is proportionate to the aim pursued and the rights of the individuals are protected.

5. DATA PROTECTION OFFICER

Data Protection Officers are specifically required in certain circumstances under the General Data Protection Regulation (2018), such as where organisations process sensitive (special category) personal data on a "large scale" or are a public body. However, under the Data Protection Act (2018), local councils (and parish councils and parish meetings) are excluded from the definition of "public authority or body". This means that local councils do not automatically have to have a Data Protection Officer unless the local council processes personal data for regular and systematic monitoring of data subjects on a large scale, or processes sensitive personal data on a large scale.

There are no definitions of "large scale" or "regular and systemic monitoring" in either the Data Protection Act (2018) or the General Data Protection Regulation (2018). However, the guidance states that:

- When assessing "large scale", consideration should be given to the number of data subjects concerned, the amount of data held about them and the type of data, how long the data is kept and the geographical extent of the processing.
- "Regular and systematic monitoring" includes all forms of tracking and profiling on the internet, although it is not restricted to the online environment and could be any ongoing monitoring of behaviour. It includes monitoring such as location tracking on mobile apps or the use of smart meters in the home. The use of CCTV to monitor people's movements (rather than just as a security measure) could also be covered.

The role of the Data Protection Officer is to assist the data controller, i.e. the parish council, or the data processor, usually the Clerk, to monitor compliance with the General Data Protection Regulation by:

- Raising data protection awareness within the council, and advising on Regulation compliance;
- Ensuring the implementation of the appropriate documentation to demonstrate Regulation compliance;
- Monitoring the implementation and compliance with policies, procedures and the Regulation in general;
- Being involved in the Council's handling of data breaches, including assisting and advising the council with its notifications to the Information Commissioner's Office and data subjects where necessary (but it is the Council which has the obligation to notify in certain circumstances not the Data Protection Officer);
- Liaising with the Information Commissioner's Office, the relevant councillors and staff and the data subjects;
- Monitoring Data Protection Impact Assessments; and
- Co-operating with and acting as the contact point for the Information Commissioner's Office on issues relating to processing.

Clerks and Responsible Financial Officers cannot be designated as a parish council's Data Protection Officer. This is because although they may satisfy some requirements of the Data Protection Officer's role, they will not satisfy all of them. There can also be a conflict of interest between the role of a Clerk and Responsible Financial Officer and that of a Data Protection Officer and these types of conflicts should be avoided.

Aside from or in place of a Data Protection Officer, a parish council may wish to appoint a staff member who is able to provide central support and guidance in respect of compliance with data protection legislation. If a staff member is to take on this role, it does not need to be a new member of staff, but may be added to the duties of an existing member of staff. The job title "Data Protection Compliance Officer" or similar, rather than "Data Protection Officer" ought to be used, to avoid

confusion with the Data Protection Officer (if there is one), to which specific responsibilities are attached under the legislation.

Recommendations

- To agree not to appoint a Data Protection Officer as Chawleigh Parish Council does not process personal data for regular and systematic monitoring of data subjects on a large scale, or process sensitive (special category) personal data on a large scale.
- To appoint a Data Protection Compliance Officer.

6. DATA PROTECTION LAW COMPLIANCE ACTION PLAN

A draft data protection law compliance action plan is set out in Appendix A. The action plan will need to be regularly monitored by the Parish Council.

Issues for consideration include:

- A series of supporting policies and procedures need to be developed.
- A cybersecurity audit needs to be undertaken to limit the risk and impact of a personal data breach.
- The Council's website is hosted by the BT Community website and information re. the use of cookies and the collection of website data including activity information and device information needs to be clarified as no analytical information has been sought or received to date.
- The Council's Parish Grant application form will need to be updated to include clear consent opt-in information.

Recommendations

- To agree the data protection law compliance action plan and to schedule update reports to the Parish Council on a regular basis.
- To approve the payment of an annual data protection fee of £40 (or £35 if paid by Direct Debit) to the Information Commissioner's Office.

7. SUMMARY OF RECOMMENDATIONS

Chawleigh Parish Council is asked:

- To agree not to appoint a Data Protection Officer as Chawleigh Parish Council does not process personal data for regular and systematic monitoring of data subjects on a large scale, or process sensitive (special category) personal data on a large scale.
- To appoint a Data Protection Compliance Officer.
- To agree the data protection law compliance action plan and to schedule update reports to the Parish Council on a regular basis.
- To approve the payment of an annual data protection fee of £40 (or £35 if paid by Direct Debit) to the Information Commissioner's Office.

8. REFERENCES

The National Association of Local Councils has published a General Data Protection Regulation Toolkit that provides guidance, as well as a number of practical tools and templates, to assist parish councils with General Data Protection Regulation compliance. A revised document was published in August 2018 to reflect the new Data Protection Act (2018) and data protection regime. The changes include the appointment of a Data Protection Officer, which is not mandatory for all local (parish and town) councils, and information about paying the Information Commissioner's data protection fee.

APPENDIX A - DATA PROTECTION LAW COMPLIANCE ACTION PLAN
Updated 10 August 2018

Ref.	Action	Lead	Due Date	Status
1.	**Raising awareness**			**Ongoing**
1.1	**Attend training** 10/08/18: Clerk attended training on: • General Data Protection Regulation 2018 provided by Devon Association of Local Councils on 19/04/18 • Data Protection Act 2018 provided by Mid Devon District Council on 30/05/18	Clerk	May 2018	Closed
1.2	**Provide a briefing to councillors** 10/08/18: Briefing document on data protection law provided for Council meeting to be held on 16 August 2018. Copy of the General Data Protection Regulation toolkit provided by the National Association of Local Councils circulated to all councillors to raise awareness of the issues around data protection law.	Clerk	16/08/18	Closed
1.3	**Decide who will be responsible for the Parish Council's compliance with data protection law** 10/08/18: A recommendation for the Parish Council to consider appointing a Data Protection Officer and/or a Data Protection Compliance Officer will be presented to the Council meeting to be held on 16 August 2018.	Councillors	16/08/18	Ongoing
1.4	**Pay a data protection fee** 10/08/18: A recommendation for the Parish Council to register with the Information Commissioner's Office will be presented to the Council meeting to be held on 16 August 2018.	Clerk	17/08/18	Ongoing
1.5	**Publish a data protection law compliance action plan and agree the reporting schedule** 10/08/18: Action plan will be presented to the Council meeting to be held on 16 August 2018.	Clerk	16/08/18	Ongoing
2	**Developing a Privacy Policy**			**Ongoing**
2.1	**Develop a Privacy Policy** 10/08/18: Draft Privacy Policy based on National Association of Local Councils template to be presented for approval at the Council meeting to be held on 16 August 2018.	Clerk	16/08/18	Ongoing
3.	**Developing Privacy Notices**			**Ongoing**
3.1	**Develop a General Privacy Notice** 10/08/18: General Privacy Notice based on National Association of Local Councils template drafted for approval at the Council meeting to be held on 16 August 2018	Clerk	16/08/18	Ongoing
3.2	**Develop a Privacy Notice for staff, councillors and role holders** 10/08/18: Privacy Notice for staff, councillors and role holders based on National Association of Local Councils template drafted for approval at the Council meeting to be held on 16 August 2018.	Clerk	16/08/18	Ongoing

Ref.	Action	Lead	Due Date	Status
4.	Undertaking a Personal Data Audit			
4.1	Develop a personal data audit questionnaire	Clerk	27/09/18	
4.2	Complete the personal data audit questionnaire	Clerk	13/12/18	
5.	Establishing a register of processing activities			
5.1	Develop a Retention and Disposal Policy	Clerk	27/09/18	
5.2	Develop a register of processing activities	Clerk	27/09/18	
5.3	Complete a register of processing activities	Clerk	13/12/18	
6.	Reviewing consent			
6.1	Refresh existing consents	Clerk	27/09/18	
6.2	Develop a new consent template	Clerk	31/01/19	
6.3	Update the Parish Grant application form	Clerk	Apr 2019	
7.	Developing a Subject Access Policy			
7.1	Develop a Subject Access Policy	Clerk	31/01/19	
8.	Developing a Security Incident Response Policy			
8.1	Develop a Security Incident Response Policy	Clerk	31/01/19	
9.	Developing a Data Protection Impact Assessment Procedure			
9.1	Develop a Data Protection Impact Assessment Procedure		TBC	
9.2	Develop Data Protection Impact Assessment checklist		TBC	
10.	Undertaking a cybersecurity review			
10.1	Develop a cybersecurity audit questionnaire		TBC	
10.2	Complete the cybersecurity audit questionnaire		TBC	
11.	Reviewing the management of the website			
11.1	Clarify the cookie policy of the BT community website		TBC	