Sway Parish Council
GDPR – Guidance and Action Plan

Prepared in May 2018 by the Parish Clerk, including excerpts from NALC GDPR Toolkit and LCAS Information Pack.

INTRODUCTION

The General Data Protection Regulation 2018 (GDPR) will take effect in the UK from 25 May 2018. It replaces the existing law on data protection (the Data Protection Act 1998) and gives individuals more rights and protection regarding how their personal data is used by councils. Local councils must comply with its requirements, just like any other organisation.

A new principle of accountability puts the compliance burden on councils, requiring them to produce and maintain documents that demonstrate what actions have been taken to achieve compliance. The new accountability principle means that we must be able to show that we are complying with the principles (see below). In essence, we cannot just state we are compliant; we have to prove it and provide evidence. To do this there are a number of actions to be completed.

This document sets out the requirements of GDPR and Sway PC's plans and processes to achieve compliance.

TERMS AND ROLES

Data controller is the person or organisation who determines the how and what of data processing.

Data processor is the person or firm that processes the data on behalf of the controller.

Data subject is the person about whom personal data is processed.

Consent is a positive, active, unambiguous confirmation of a data subject's agreement to have their data processed for a particular purpose. Consent must be easy to withdraw and must be freely given, provided on an opt- in basis rather than opt-out.

Personal data is information about a living individual which is capable of identifying that individual e.g. a name, email address or photo.

Privacy Notice is a notice from a data controller to a data subject describing how personal data will be used and what rights the data subject has.

Processing is anything done with/to personal data (obtaining, recording, adapting or holding/storing) personal data.

Sensitive personal data is also described in the GDPR as 'special categories of data' and is the following types of personal data about a data subject: racial or ethnic origin; political opinions; religious beliefs; trade union membership; physical or mental health or condition; sexual life or orientation; genetic data; and biometric data.

Sway Parish Council
GDPR – Guidance and Action Plan

Prepared in May 2018 by the Parish Clerk, including excerpts from NALC GDPR Toolkit and LCAS Information Pack.

Data Protection Officer (DPO) assists the controller or the processor to monitor internal compliance with this Regulation, provides guidance and training, carries out audits and acts as contact point to the Information Commissioner's Office (ICO). The Govt confirms that Parish Councils will be exempt from having to appoint a DPO.

Allocated Roles:

- Data Controller: Sway Parish Council
- Data Processor: Parish Clerk, Payroll Service, Allotment Committee, Councillors
- Data Subject: residents, allotment holders, staff, councillors

MAIN CHANGES AND IMPACTS OF THE GDPR

One of the main changes to note is that the GDPR places a much greater emphasis on transparency, openness and the documents we need to keep in order to show that we are complying with the legislation. This is incorporated within the idea of 'accountability'.

The GDPR will however impose new burdens on councils, including new reporting requirements and increased fines and penalties. The UK Government has made clear that after Brexit the UK will continue to adopt a similar standard for data protection as set out in the GDPR.

CHANGE	DETAILS	IMPACT
Record Keeping	Each Data Controller must maintain a record of processing activities under its responsibility. Data Processors must also keep a record of the processing activities they carry out on behalf of a Data Controller.	The level of detail is the same as contained in an ICO registration / notification at present and the log can be requested at any time by the ICO.
Privacy Notices	Under the GDPR, privacy notices must contain more information, be more transparent, use clear and plain language, and must be easily accessible.	Privacy notices will need to be reviewed and updated to make them clearer, more transparent and easily accessible.

Sway Parish Council
GDPR – Guidance and Action Plan

Prepared in May 2018 by the Parish Clerk, including excerpts from NALC GDPR Toolkit and LCAS Information Pack.

CHANGE	DETAILS	IMPACT
Consent	The way consent is obtained will change under the GDPR as individuals have more rights to decide how their data is processed. Where processing personal data is based on consent, the council must be able to evidence the consent. Consent must be by an "opt in" method.	The types of processing activities which require the consent of an individual need to be identified and consents must be captured in a GDPR compliant manner.
Breaches	Data Controllers must report personal certain types of data breaches to the ICO without 'undue delay', and where possible no later than 72 hours after having become aware of the breach. An individual who has suffered damage as a result of a breach can claim compensation from the Data Controller or the Data Processor.	How councils handle data breaches should be reviewed. Training will be required to increase awareness of what constitutes a breach and how to escalate investigations into breaches.
Right of Access (Subject Access Requests)	The time limit to comply with a Subject Access Request ("SAR") has been reduced from 40 calendar days to one calendar month. The ability to charge £10 per SAR has been removed so all SARs are free of charge from 25th May 2018.	The SAR process will need to be reviewed and updated accordingly.
Data Privacy Impact Assessments (DPIA)	The GDPR makes it mandatory for DPIAs to be carried out in certain situations. DPIAs will need to contain a description of the processing and the purpose of the processing and need to identify any risks to the personal data and the rights and freedoms of individuals, and the measures and safeguards implemented to mitigate these risks.	DPIAs will need to be introduced where new technologies are used (e.g. CCTV or other monitoring) for high risk data processing activities (e.g. large-scale processing of sensitive personal data) or when there are systematic and extensive activities which use automated processing to evaluate, analyse or predict behaviour (e.g. tracking behaviour on a website).

Sway Parish Council
GDPR – Guidance and Action Plan

Prepared in May 2018 by the Parish Clerk, including excerpts from NALC GDPR Toolkit and LCAS Information Pack.

CHANGE	DETAILS	IMPACT
Privacy by Design	When developing, designing or using services or applications which involve processing personal data, Data Controllers and Processors should adopt internal policies and measures to ensure personal data is protected.	If councils introduce new IT systems or launch new websites which collect personal data these new systems should have data protection controls built into their designs from the outset.
Right to Object to data processing	Individuals must be advised of their right to opt out of processing activities, including marketing.	'Unsubscribe' methods will need to be reviewed. Any reasonable requests to object to processing should be stored and evidenced.
Right to Erasure	An individual has a right to request that their personal data is deleted. A Data Controller must delete personal data unless there is a legal obligation to retain the personal data.	Data deletion processes will need to be introduced so that data is not retained indefinitely. It's likely a 'data cleansing' exercise will need to be carried out prior to 25th May 2018 so that the council is not storing data it no longer requires or has a need to retain.
Profiling	An individual has the right not to be subject to a decision based solely on 'automated processing', including profiling. This is where a computer, or computer software rather than a human makes a decision about an individual.	Activities that rely or use automated decision making need to be identified. Processes need to be put in place to allow, where possible, individuals to object to automated decision making (and e.g. request that a human intervenes to make the decision).
Right of Portability	The GDPR introduces a new right of data portability. This right allows for the data which an individual provided to the Data Controller to be provided to the individual in a structured format, to allow it to be provided to another Data Controller.	It will be important to understand where the data is being stored and in what format to make it easier to move personal data (and receive personal data from other data controllers).

Sway Parish Council
GDPR – Guidance and Action Plan

Prepared in May 2018 by the Parish Clerk, including excerpts from NALC GDPR Toolkit and LCAS Information Pack.

MAIN PRINCIPLES OF THE GDPR

The GDPR has a number of underlying principles. These include that personal data:

- Must be processed lawfully, fairly and transparently.
- Is only used for a specific processing purpose that the data subject has been made aware of and no other, without further consent.
- Should be adequate, relevant and limited i.e. only the minimum amount of data should be kept for specific processing.
- Must be accurate and where necessary kept up to date.
- Should not be stored for longer than is necessary, and that storage is safe and secure.
- Should be processed in a manner that ensures appropriate security and protection.

SWAY PC ACTION PLAN

ACTION	COMMENTS
Data audit (including identification of lawful basis for data processing)	Completed
Risk assess current data processes	Completed
Obtain appropriate consent	Completed
Provide suitable privacy notices	Completed
Create a Data Access Policy	Completed
Update Data Protection Policy	Completed
Create a process for security breach response	To be drafted and approved