STAINFORTH PARISH COUNCIL (North Yorkshire)

GENERAL DATA PROTECTION REGULATIONS – 25TH MAY 2018 P1

The key areas identified below are designed to highlight the main points of compliance to the regulations, and their implications to the Parish Council.

Data Audit

Information Held	Where Held	Third Party (Shared)	Permission
Clerk contact Information	Stainforth.info (village) website & documentation	Freely available	Yes
Clerk contract of employment	Hard copy (locked cabinet)	Available to Parish Council only	Yes
Councillors details	Website Hard copy files (locked cabinet)	Freely available on web No hard copy shared	Yes
E-mail Contacts	UK2 account (password protect)	None Use of BCC	Ongoing
Electoral Roll	Hard Copy File (locked Cabinet)	Craven District Council	Completion of Electoral roll.
Invoice - Business Names	Included in finance statements on website Laptop & back up storage (encrypted)	Displayed on website. Transparency	Ongoing
Planning Applications	Hard copies (locked cabinet) after 6 months destroyed.	All planning applications & decisions freely available on Planning authority website	By submission of planning application.
Names for business purposes on bank statements.	Hard Copy (locked cabinet) Laptop & backup storage (encrypted)	Made available for internal audit purposes annually.	Ongoing

Processing Data

Stainforth Parish Council has statutory liabilities in respect to transparency and accountability of public finance, and this involves the processing of information.

All business transactions involving receipt or payment by the Parish Council will be recorded on a monthly Financial Statement and displayed on the Council website, this is inclusive of all business names used for receipt or invoice purposes. All correspondence leading to a business transaction between the Parish Council and a contractor will receive a permission statement for their attention.

Example: ***All financial business transactions with Stainforth Parish Council will be recorded and displayed on their website, this is a legislative responsibility of the Council in regard to transparency and accountability of public finance. Any name and amount as it appears on an invoice will be displayed to satisfy this responsibility, please contact the Parish Clerk if this practice is unacceptable to you.***

STAINFORTH PARISH COUNCIL (North Yorkshire)

GENERAL DATA PROTECTION REGULATIONS – 25TH MAY 2018 P2

Subject Access requests

Individuals have the right to know what data is held on them, why the data is being processed and whether it will be given to any third party. They have the right to be given this information in a permanent form (hard copy). This is known as a 'Subject Access Request' (SAR).

The Parish Council must comply with an SAR within one month of the request, and the hard copy information must be free of charge.

Emails

Each contact held by the Parish Clerk on behalf of the Council in relation to its business will be emailed with a 'consent to be contacted' attached, the recipient will need to respond with their permission, to enable further contact from the Clerk on behalf of the Parish Council.

Councillors

To be aware of the GDPR and its implications on the Parish Council, this document is designed to raise awareness of the regulations and identify the key areas of compliance. The Clerk has the role of processing information on behalf of the Council and therefore inherits the responsibility of managing data effectively and in compliance with the GDPR.

Note:

When Councillors use Email to send a message conducting any Council business to more than one contact (except Councillors & Clerk), it is recommended to use the Blind Carbon Copy (BCC) facility, thus avoiding third party access to their contacts.

Personal Data Breaches

A data breach is a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the Parish Council has incorporated measures to protect against such a data breach.

If there is no risk of harm to an individual (for example because some low risk data has been inadvertently released or made public, such as an Email address, then this need not be reported. Unless the data released could be used to steal someone's identity, such as their banking data, this should be reported to the Information Commissioners Office (ICO).

Examples of personal data breaches and how to avoid them:

1. Emails and attachments being sent to the wrong person, or several people – Slow down & check before sending.
2. The wrong people being copied into Emails and attachments – Use Blind Carbon Copy (BCC).
3. Malware (IT) – Ensuring up to date anti-virus installed.
4. Laptop theft – Ensure encryption.

Any data breach report can be facilitated through the Information Commissioners Website www.ico.org.uk

Peter Leng
Clerk & RFO – Stainforth Parish Council (North Yorkshire)