GENERAL DATA PROTECTION REGULATIONS *(GDPR)* OVERVIEW

As of the 25th May 2018, businesses across the EU will be required to follow General Data Protection Regulations (GDPR), which will be replacing the Data Protection Act (DPA). GDPR has been introduced to ensure new strict regulations surrounding data protection and will improve transparency, fairness and lawful processing of everyone's personal data.

The increasing use of information technology means that more personal data is being collected, stored and used by organisations and on a global scale. This means there is an ever-increasing risk of loss or misuse. This will have implications for not just our parishioners but also all our employees and contractors information too.

The following information will help you understand the changes and processes required to comply with these new rules.

OBJECTIVES

The main objectives of this document are to help you understand the following:

- Key concepts and terminology of GDPR.
- The importance of protecting personal data and identify which information this applies to.
- The principles of data protection.
- The importance of Data Subjects under the Act.
- The responsibilities of Data Controllers.
- The consequences of non-compliance.

WHAT IS GDPR?

The EU General Data Protection Regulation (GDPR) is intended to establish one single set of rules across Europe, making it simpler for organisations to do business across the Union. **This includes organisations outside the EU who process the data of EU citizens**.

The GDPR governs how all personal data is processed and places specific responsibilities and duties on you and your organisation, if personal data is used.

WHAT INFORMATION DOES THIS APPLY TO?

The GDPR applies to 'personal data', meaning any information relating to an individual person.

Personal Data in particular applies to:

- Names & Addresses
- Contact Information – Telephone Numbers / Email Addresses
- Financial Details (including bank details)
- Photos
- Salary, Tax & Pension Details
- Health & Safety Reports (accident reports)
- Sickness Records & Medical Information
- CV's & Job Applications
- Holiday Requests & Disciplinary Procedures

Special Category Data is personal data which the GDPR regard as more sensitive, therefore are subject to additional protections. Special Category Data includes information about an individual's:

- Racial of Ethnic Origin
- Religious or Philosophical Beliefs
- Trade-Union Memberships
- Health or Sexuality

WHAT DOES THIS MEAN FOR EVERYONE?

Under GDPR, organisations must take careful considerations when storing personal data. The GDPR applies to both automated personal data and to manual filing systems, where personal data are accessible according to specific criteria.

- **Automated** personal data is information processed or intended to be processed, wholly or partly by automatic means, e.g. practice management systems.
- **Manual** filing systems is information processed in a non-automated manner, which forms part of or is intended to form part of, a 'filing system', e.g. employee contracts.

As more organisations hold data on IT and communications systems and with more sophisticated tracking of consumer preferences on search engines and websites, threats on privacy have become a main concern.

- **Unintentional Actions** – leaving data where it can be easily seen, hardware or software crashes or failures and disclosing information without prior approval, e.g. leaving computer logged in and unattended.
- **Intentional Actions** – a person can intentionally misuse personal information, e.g. changing details without authorisation, stealing data or using bribery to extract data.
- **Crime** – malicious software such as malware or viruses and/or action by criminals can expose weaknesses in computer systems and result in data loss.

ROLES, RIGHTS & RESPONSIBILITIES

DATA SUBJECT – a data subject is any living individual that the personal data relates to. **We are all Data Subjects**. Whenever you book a flight, use a credit card or browse on the Internet, you disclose some personal data and an organisation may store information about you. Data Subjects can be parishioners, suppliers,

clients, customers or any other person about whom information is held. It also includes current employees, job applicants or former employees.

GDPR upholds fundamental rights for anyone who has personal data stored by your organisation.

DATA CONTROLLER – the data controller is an individual or organisation, in this case **Eastington Parish Council**, who determines the purpose and manner in which any personal data is processed. Controllers are responsible for ensuring that any processing activities are performed in compliance with the EU data protection law. Controllers must implement appropriate technical and organisational measures, not only to ensure compliance, but also to demonstrate that measures are in place. This responsibility lies with not only Eastington Parish Council, but also its staff.

Data Controllers Responsibilities:

- To remain up to date and continually review data protection legislation
- Monitor and control what data is collected
- Why this data was collected and whether it is still needed

DATA PROCESSOR - a data processor is a separate organisation or individual (Parish Clerk) that processes personal data on behalf of the Data Controller. This could include:

- IT Services (e.g. website and HCI data)
- CCTV
- External – SDC, GCC, Police
- Lloyds bank

DATA PROTECTION OFFICER – a Data Protection Officer (DPO) ensures that an organisation complies with its data protection regulations. This can be the Parish Clerk; however legislation changes exempt parish councils from the requirement of appointment a DPO.

REGULATION & ENFORCEMENT

The Data Protection Principles provide the conditions in which an organisation is permitted to process personal data. Organisations need to ensure that their data processing activities are carried out in accordance with the Data Protection Principles to avoid any unauthorised processing.

- **Fair, Lawful & Transparent** – personal data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. It requires that organisations take additional care when designing and implementing data processing activities.

- **Purpose Limitation** – personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes.

- **Data Minimisation** – personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed.

- **Accuracy** – personal data must be accurate and kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate are either erased or rectified without delay.

- **Storage Limitation** – personal data must be kept in a form that permits identification of Data Subjects for no longer than is necessary. There are specific provisions on the processing of personal data for historical, statistical or scientific purposes.

- **Integrity and Confidentiality** – personal data must be processed in a manner that ensures appropriate security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

- **Accountability** – the requirements of the accountability principle is to demonstrate compliance with the principles and states explicitly that this is the data controller's responsibility. The accountability principle ensures that organisations will still need to keep a record of how they comply with their obligations.

Despite implementing GDPR safeguards, data breaches can still occur. A personal data breach means a security breach leading to the destruction, alteration or unauthorised access to, personal data.

WHAT MUST BE DONE IF THERE IS A BREACH?

Report any potential data breach to the Parish Clerk. You will then receive further instructions of how to proceed.

Failing to notify a breach when required to do so, can result in a significant fine.

In recent years, there have been numerous incidents where personal data has been stolen, lost or subject to unauthorised access. By following some basic guidelines, you can help prevent security breaches and unauthorised access.

- Password Protection
- Locked Record / Filing Cabinets
- Log Off / Lock Unattended Computers
- Report Suspicious Cyber Incidents
- Secure the Premises
- Don't Provide Personal Information Over the Phone
- Destroy Records (where applicable)
- IT Security Protection (e.g. Anti-Virus & Malware)

The Information Commissioner's Office (ICO), which is a non-departmental public body with reports directly to Parliament, has the power to take action against those it believes have not complied with the data protection legislation.

Main Offences:

- Obtaining, disclosing, selling or offering to sell personal data without consent
- Breaching formal instruction and advice issued by Eastington Parish Council

Penalties:

- Criminal prosecution for serious breaches or non-criminal enforcement
- Audits to check organisations are complying
- Monetary penalties

If you are in doubt about any of the above please contact clerk@eastington-pc.gov.uk.