East Dean & Friston Parish Council

Date: **2nd November 2017**

Title: **Report Item 10 – General Data Protection**

By: **K Larkin (Parish Clerk)**

Purpose: **To commence council compliance with the General Data Protection Regulation (to be effective from May 2018)**

Recommendations:
a) To note the report
b) To appoint a Data Controller
c) To approve a Data Protection Policy
d) To approve an Email and Internet Usage policy

The clerk has attended training on the new General Data Protection Regulation, provided by the East Sussex Association of Local Councils. The regulation will come into force in May 2018 and councils need to be making preparations now.

The new regulation embodies eight controlling principles, which take account of the fact that with the passing of the age of paper records, and increasing reliance on digital communications and data storage, it is much easier than it used to be for personal information to 'escape' into the web where it may be passed around in an uncontrolled way and put to misuse. Personal data must therefore be handled with increasing care and sensitivity, and should wherever possible be removed from storage, leaving the individual with the 'right to be forgotten'. The eight principles are as follows:

1. Personal data must be processed fairly and legally. The council must make clear why it is collecting the data, and what it intends to do with it.
2. Personal data must only be obtained for specified and legal purposes, and must only be processed in a way that is consistent with the specified purpose. The loss of sensitive personal data, or its improper release, will in future lead to heavy fines.
3. Personal data must be adequate, relevant and not excessive for the purpose it is processed for
4. Personal data must be accurate and, where necessary, kept up to date
5. Personal data processed for any purpose must not be kept longer than is necessary to fulfil that purpose.
6. Personal data must be processed in line with the data subject's rights
7. Appropriate security measures must be taken to protect against unauthorised or illegal data processing
8. Transferring personal data outside of the European Economic Area is restricted unless the rights and freedom of data subjects are protected

In order to comply with these requirements, the council must take the following actions:

- Appoint a Data Controller
- Adopt a suitable Data Protection policy (a draft supplied by SALC is appended to this report, pages 3-5). This policy, like all policies, will be public.
- Privacy notices must accompany all communications, stating that '*Any personal information such as name, postal address, telephone number, and email address given via this website will only be used to provide a requested service and will not be disclosed to any other third party without your prior permission or unless we are required to do so by law'.*
- 'Direct marketing' (this includes email circulars and newsletters) can only be done with consent. People should be invited to register to opt in to continued communication, and asked to specify how they would like to be contacted. A means of opting out should always be clearly offered and easy to use (e.g. a tick box). A draft Email and Internet Usage policy is appended to this report (pages 6-8)
- Data audit and cleansing - Councils need to undertake an audit of their records to establish what personal data they are holding, and then to securely destroy any that is no longer strictly needed. It is suggested that the clerk should commence the audit and report back. This exercise will need to be repeated at regular intervals and with complete transparency. The Data Protection policy should make clear what the procedure is, and what the regular review period should be.
- Training should be undertaken by all councillors and officers in IT security, with special reference to the oversight of portable equipment and removable media.
- Processes need to be put in place to evaluate new projects from a data protection point of view.

Appendix

DRAFT DATA PROTECTION POLICY

1. Introduction

1.1 The council holds and processes information about employees, councillors, residents and customers, and other data subjects for administrative and commercial purposes.

1.2 When handling such information the council, and all staff or others who process or use the information, must comply with the Data Protection principles as set out in the Data Protection Act 1998 (the Act).

2. Data protection principles

2.1 There are eight principles set out in the Act, which in summary state that data shall:

- be processed fairly and lawfully
- be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with the purpose
- be adequate, relevant and not excessive for the purpose
- be accurate and up-to-date
- not be kept for longer than necessary for the purpose
- be processed in accordance with the Data Subject's rights
- be kept safe from unauthorised processing, and accidental loss, damage or destruction
- not be transferred to a country outside the European Economic Area, unless that country has the equivalent levels of protection for personal data, except in specified circumstances

3. Responsibilities

3.1 **[ENTER NAME]** Council is the Data Controller and must ensure that any processing of personal data for which they are responsible complies with the Act.

3.2 The Data Protection Officer is the Clerk, who acts on behalf of the council, and is responsible for:

- fully observing conditions regarding the fair collection and use of information
- meeting the Council's legal obligations to specify the purposes for which information is used
- collecting and processing relevant information, only to the extent that is required to fulfil operational needs/to comply with legal requirements
- ensuring the quality of information used
- applying strict checks to determine the length of time that information is held
- ensuring that the rights of the people whom information is held are able to be fully exercised under the Act
- taking appropriate technical and organisational security measures to safeguard personal information
- ensuring that personal information is not transferred abroad without suitable safeguards
- ensuring that everyone managing and handling personal information
    - full understands that they are contractually responsible for following good practice in terms of protection
    - is adequately trained to do so
    - are appropriately supervised

4. Storage and retention

4.1 Personal data is kept in paper-based systems and/or on a password-protected computer system.

4.2 The council will keep different types of information for differing lengths of time, depending on legal and operational requirements. More information can be found in the council's Document Retention Scheme.

5. Access to information

5.1 Any employees, councillors, residents, customers and other data subjects have a right to:

- ask what personal information the council holds
- ask what this information is used for
- be provided with a copy of the information
- be given details of the purposes for which the council uses the information and any other persons organisations to whom it is disclosed

- ask that any incorrect data held is corrected

5.2 If it is felt by the data subject that any personal information held is incorrect the individual may request that it be amended. The council must advise the individual within 21 days whether or not the amendment has been made.

6. Breach of policy

6.1 Compliance with the Act is the responsibility of all councillors, residents, customers and members of staff. Any deliberate or reckless breach of the policy may lead to disciplinary action and where appropriate, legal proceedings.

6.2 Any individual who believes that the council has breached any of the requirements of the Data Protection Act 1998 should raise the matter with the Clerk. Alternatively, a complaint can be made to the Information Commissioner, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

DRAFT EMAIL AND INTERNET USAGE POLICY

7. Introduction

7.1 The council recognises that email and internet are important information and communication systems which are used during the course of council business. This policy provides guidelines and procedures to protect users and the council.

7.2 This policy applies to all staff members who have access to the internet and email facilities via council computers.

7.3 The email policy applies to all councillors in their correspondence with staff members and/or other councillors.

8. Internet usage

8.1 Staff members are encouraged to use the internet responsibly as part of their official and professional activities.

8.2 Information obtained via the internet and published in the name of the council must be relevant and professional. A disclaimer must be stated where personal views are expressed.

8.3 The use of the internet to access and/or distribute any kind of offensive material will not be tolerated and staff may be subject to disciplinary action.

8.4 The equipment, services and technology used to access the internet are the property of the council. The council reserves the right to monitor internet traffic and monitor and access data that is composed, sent or received through its online connections.

9. Unacceptable use of the internet

9.1 Unacceptable use of the internet by staff members includes, but is not limited to:

- sending or posting discriminatory, harassing or threatening messages or images
- using computers to perpetrate any form of fraud, and/or software, film or music piracy
- obtaining, using or disclosing another staff member's password without authorisation

- sharing confidential material or proprietary information outside of the council
- hacking into unauthorised websites
- sending or posting information that is defamatory to the council, its services, councillors and/or members of the public
- introducing malicious software onto council computers and/or jeopardising the security of the council's electronic communication systems
- sending or posting chain letters, solicitations or advertisements not related to council business or activities
- passing off personal views as those representing the council
- accessing inappropriate internet sites, web pages or chat rooms

9.2 If a staff member is unsure about what constitutes acceptable internet usage, then he/she should ask his/her line manager for further guidance and clarification

10. Email

10.1 Use of email is encouraged as it provides an efficient system of communication.

10.2 Email should be regarded as written paper documents for the purposes of production, use, retention and disclosure and can be called upon under the Freedom of Information Act 2000. Personal information should be kept in accordance with the principles established in the Data Protection Act 1998.

10.3 The council reserves the right to open any email file stored on the council's computer system.

10.4 The following guidelines for email use should be observed by all staff members and councillors:

- use appropriate language to avoid unintentional misunderstandings
- respect the confidentiality of information contained within emails, even if encountered inadvertently
- check with the sender if there is any doubt regarding the authenticity of a message
- do not open any attachment unless certain of the authenticity of the sender
- only copy emails to others where appropriate and necessary

- emails which create obligations or give instructions on behalf of the council must be sent by officers only, not councillors
- emails must comply with common codes of courtesy, decency and privacy

11. Reporting and sanctions

11.1 If a councillor receives an email from a staff member which they believe is contrary to the guidance provided in this policy, it should be reported to the Clerk who will consider use of the council's formal disciplinary procedure, or refer the matter to the **[ENTER COMMITTEE OR COUNCIL]** depending on the severity of the event.

11.2 If a staff member receives an email from another staff member which they believe is contrary to the guidance provided in this policy, it should be reported to the Clerk who will consider use of the council's formal disciplinary procedure, or refer the matter to the **[ENTER COMMITTEE OR COUNCIL]** depending on the severity of the event.

11.3 If a staff member receives an email from a councillor which they believe is contrary to the guidance provided in this policy, the staff member is entitled to consider use of the council's grievance policy and/or report the issue through the procedures outlined in the Member's Code of Conduct.

12. Security

12.1 Only software purchased by the council shall be installed on the council's computer system. Software licences shall be retained.