Appendix L

Agenda Item: **11.1**

Report to: **Finance & Human Resources Committee**

Date: **Wednesday 27th January 2020**

Subject: **GDPR Responsibilities**

Summary: Setting out responsibilities of the corporate body

Decisions Required:

To note and consider the responsibilities of the corporate body in relation to data protection and present to Full Council.

There are many new policies taking into account data protection rules and regulations. This report has taken out the main responsibilities of the corporate body for you to understand and analyse.

1. GDPR and Data Protection Act 2018

The Act works in two ways. Firstly, it states that anyone who processes personal information must comply with six principles (Article 5 of the GDPR), which make sure that personal information is:

a) processed lawfully, fairly and in a transparent manner
b) collected and processed for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those original purposes
c) Adequate, relevant, and limited to what is necessary for the purpose
d) Accurate and kept up to date
e) Not kept for longer than is necessary and subject to appropriate technical and organisational measures to safeguard the rights and freedoms of individuals
f) processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing; and

Secondly, it provides individuals with important rights (Articles 13 and 14):

1) Right to be informed
2) Right of access
3) Right to rectification
4) Right to erasure (right to be forgotten)
5) Right to restrict processing
6) Right to data portability
7) Right to object
8) Rights related to automated decision making including profiling

2. CCTV Policy

Responsibilities

The Parish Council, as a legal entity, retains overall responsibility and will:

- Ensure that the use of CCTV systems is implemented in accordance with this policy.
- Oversee and co-ordinate the use of CCTV monitoring for safety and security purposes within the Parish Council premises.
- Ensure that all existing CCTV monitoring systems will be evaluated for compliance with this policy.
- Ensure that the CCTV monitoring is consistent with the highest standards and protections.
- Review camera locations and be responsible for the release of any information or recorded CCTV materials stored in compliance with this policy.
- Maintain a record of access (e.g. an access log) to or the release of tapes or any material recorded or stored in the system.
- Ensure that monitoring recorded tapes are not duplicated for release.
- Ensure that the perimeter of view from fixed location cameras conforms to this policy both internally and externally.
- Give consideration to both Parish Council members and staff feedback/complaints regarding possible invasion of privacy or confidentiality due to the location of a particular CCTV camera or associated equipment.
- Ensure that all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals within the Parish Council and be mindful that no such infringement is likely to take place.
- Ensure that external cameras are non-intrusive in terms of their positions and views of neighbouring residential housing and comply with the principle of "Reasonable Expectation of Privacy"
- Ensure that monitoring tapes are stored in a secure place with access by authorised personnel only
- Ensure that images recorded on tapes/DVDs/digital recordings are stored for a period not longer than 31 days and are then erased unless required as part of a criminal investigation or court proceedings (criminal or civil) or other bona fide use as approved by Parish Council members.
- Ensure that when a zoom facility on a camera is being used, there is a second person present with the operator of the camera to guarantee that there is no unwarranted invasion of privacy.
- Ensure that camera control is solely to monitor suspicious behaviour, criminal damage etc. and not to monitor individual characteristics.
- Ensure that camera control is not infringing an individual's reasonable expectation of privacy in public areas.

CCTV Signage

It is a requirement of the Data Protection Act to notify people entering a CCTV protected area that the area is monitored by CCTV and that pictures are recorded. The Parish Council is to ensure that this requirement is fulfilled. The CCTV sign should include the following:

- That the area is covered by CCTV surveillance and pictures are recorded.
- The purposes of using CCTV.
- The name of the Parish Council.
- The contact telephone number or address for enquiries.

3. Data Protection Policy

All individuals permitted to access personal data in line with their work duties must agree to comply with this policy and agree to undertake any relevant training that may be appropriate to the role being undertaken.

The obligations outlined in this policy apply to everyone who has access to, holds copies of or processes personal data. This includes those who work at/from home or have remote or flexible patterns of working.

Data Protection Officer

The Data Protection Officer will provide an annual report of their activities and, where relevant, report to the committee their advice and recommendations on Parish Council data protection issues.

Responsibilities

Anyone processing personal data must comply with the principles of good practice. These principles are legally enforceable and can be summarised as follows:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals;

2. Obtained for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

3. Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed;

4. Accurate and kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the

purposes for which they are processed, are erased, or rectified without delay;

5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures. In accordance with the rights of data subjects under the GDPR and DPA.

External agencies or companies contracted to undertake processing of personal data on behalf of the Parish Council must demonstrate, via a written agreement, that personal information belonging to the Parish Council will be handled in compliance with the GDPR and DPA and that it has the necessary technical and organisational security measures in place to ensure this.

All printout material, magnetic tape, diskettes, CD's or DVD's, manual files, hand written notes etc, which contain personal data and are no longer required, will be treated as confidential waste, and disposed of securely.

The Parish Council will use a Data Protection Impact Assessment (DPIA) toolkit to evaluate all new computer systems to help it determine how data protection compliance can be assured. In addition, all existing systems will be subject to periodic assessment.

DPIA toolkits provide a step-by-step approach to evaluate the test proposed, new or existing information systems for compliance with the legislation. The DPIA process helps to identify weaknesses or risks to data losses or breaches and consider action that needs to be taken to ensure compliance where such compliance is not yet achieved. DPIA applies equally to paper as well as electronic data holding systems.

Training and awareness

Data Protection training and awareness is crucial so that all staff understand their responsibilities relating to data protection and the use of personal data. Failure to comply with the GDPR, DPA and the principles could lead to serious problems, and in some cases may result in significant fines or criminal prosecution.

It is the Parish Council's policy that all members and staff complete the applicable training annually. This includes employees that do not have internet or email access. The Clerk and Responsible Officer will be responsible for ensuring that staff without internet or email access receive appropriate training.

4. Freedom of Information Policy

Overall responsibility for ensuring that the Parish Council meets the statutory requirements of the FOIA, EIR and DPA lies with the Clerk and Responsible Officer and the Committee Members who have overall responsibility for information management issues. They have delegated the day-to-day responsibility of implementation to the Clerk and Responsible Officer.

The Clerk and Responsible Officer and the Committee Members are required to ensure that the Parish Council have in place adequate guidance on FOI and effective measures to comply with this policy.

Third parties who are users of information supplied by the Parish Council will be required to confirm that they will abide by the requirements of the FOIA and indemnify the Parish Council against any prosecutions, claims, proceedings, actions or payment of compensation or damages, without limitation.

The Parish Council will ensure that:

- Everyone managing, and handling information understands that they are responsible for following good information management practice;
- Staff who handle information are appropriately supervised and trained;
- Methods of handling information are regularly assessed and evaluated;
- Any disclosure of data will be in compliance with approved procedures;
- All necessary steps will be taken to ensure that data is kept secure at all times against unauthorised or unlawful loss or disclosure;
- All contractors who are users of information supplied by the Parish Council will be required to confirm that they will comply with the requirements of the Act with regard to information supplied by the Parish Council; and
- The Parish Council will abide by any Code of Practice on the discharge of the functions of Public authorities with is issued by the Ministry of Justice. In addition, the Parish Council will take account of any guidance which is issued by the Information Commissioner to promote good practice.

5. Information Security Policy

This policy applies to all members of staff/members/committee members, including temporary workers, contractors, volunteers and any and all third parties authorised to use the IT systems. All members of staff/members/committee members are required to familiarise themselves

with its content and comply with provisions contained in it. Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the Parish Council's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

The Parish Council is committed to maintaining and improving information security and minimising its exposure to risks. It is the policy of the Parish Council to use all reasonable, practical and cost-effective measures to ensure that:

- Information will be protected against unauthorised access and disclosure
- The confidentiality of information will be assured
- The integrity and quality of information will be maintained
- Authorised staff/committee members, when required, will have access to relevant Parish Council systems and information
- Business continuity and disaster recovery plans for all critical activities will be produced, tested and maintained
- Access to information and information processing facilities by third parties will be strictly controlled with detailed responsibilities written into contract/ documented agreements
- All breaches of information and cyber security, actual and suspected, will be reported and investigated. Corrective action will be taken.
- Information security training will be available to staff/committee members on request

Non-compliance with this policy could have a significant effect on the efficient operation of the Parish Council and may result in financial loss and embarrassment.

Physical security and procedures.

Paper records and documents containing personal information, sensitive personal information, and confidential information shall be positioned in a way to avoid them being viewed by people passing by as much as possible, e.g. through windows. At the end of the working day, or when you leave your desk unoccupied, all paper documents shall be securely locked away to avoid unauthorised access.

Available locked filing cabinets and locked cupboards shall be used to store paper records when not in use.

Paper documents containing confidential personal information should not be left on office desks, on meeting tables, or pinned to noticeboards where there is general access unless there is legal reason to do so and/or relevant consents have been obtained. You should take particular care if documents have to be taken out of Parish Council owned buildings.

Roles and Responsibilities

It is the responsibility of each member of staff/committee member to adhere to this policy, standards and procedures. It is the Parish Council's responsibility to ensure the security of their information, ICT assets and data. All members of the Parish Council have a role to play in information security.

The Clerk and Responsible Officer in conjunction with councillors and IT consultant shall be responsible for the following:

a) ensuring that all IT Systems are assessed and deemed suitable for compliance with the Parish Council's security requirements;
b) ensuring that IT Security standards within the Parish Council are effectively implemented and regularly reviewed, working in consultation with the Parish Council's management, and reporting the outcome of such reviews to the Parish Council's management;
c) ensuring that all members of staff/committee members are kept aware of this policy and of all related legislation, regulations, and other relevant rules whether now or in the future in force, including, but not limited to, the GDPR and the Computer Misuse Act 1990.

The Clerk and Responsible Officer in conjunction with councillors and IT consultant shall be responsible for the following:

a) ensuring that all IT Systems are assessed and deemed suitable for compliance with the Parish Council's security requirements;
b) ensuring that IT Security standards within the Parish Council are effectively implemented and regularly reviewed, working in consultation with the Parish Council's management, and reporting the outcome of such reviews to the Parish Council's management;
c) ensuring that all members of staff/committee members are kept aware of this policy and of all related legislation, regulations, and other relevant rules whether now or in the future in force, including, but not limited to, the GDPR and the Computer Misuse Act 1990.

Furthermore, the IT Consultant, in conjunction with the Clerk and Responsible Officer and councillors shall be responsible for the following:

a) assisting all members of staff/councillors in understanding and complying with this policy;
b) providing all members of staff/councillors with appropriate support and training in IT Security matters and use of IT Systems;
c) ensuring that all members of staff/councillors are granted levels of access to IT Systems that are appropriate for each member, taking into account their job role, responsibilities, and any special security requirements;
d) receiving and handling all reports relating to IT Security matters and taking appropriate action in response [including, in the event that any reports relating to personal data, informing the Clerk and Responsible Officer];

e) taking proactive action, where possible, to establish and implement IT security procedures and raise awareness among members of staff/councillors;
f) monitoring all IT security within the Parish Council and taking all necessary action to implement this policy and any changes made to this policy in the future; and
g) ensuring that regular backups are taken of all data stored within the IT Systems at regular intervals and that such backups are stored at a suitable location offsite.

All Staff/councillors

All members of staff/councillors must comply with all relevant parts of this policy at all times when using the IT Systems.

Computers and other electronic devices should be locked when not in use to minimise the accidental loss or disclosure.

Staff/councillors must immediately inform the Clerk and Responsible Officer of any and all security concerns relating to the IT Systems which could or has led to a data breach as set out in the Breach Notification Policy.

Any other technical problems (including, but not limited to, hardware failures and software errors) which may occur on the IT Systems shall be reported to the Clerk and Responsible Officer immediately.

You are not entitled to install any software of your own without the approval of the Clerk and Responsible Officer. Any software belonging to you must be approved by the Clerk and Responsible Officer and may only be installed where that installation poses no security risk to the IT Systems and where the installation would not breach any licence agreements to which that software may be subject. Prior to installation of any software onto the IT Systems, you must obtain written permission by the Clerk and Responsible Officer. This permission must clearly state which software you may install, and onto which computer(s) or device(s) it may be installed.

Physical media (e.g. USB memory sticks or disks of any kind) may not be used for transferring files. The Clerk and Responsible Officer's approval must be obtained prior to transferring of files using cloud storage systems.

If you detect any virus this must be reported immediately to the Clerk and Responsible Officer (this rule shall apply even where the anti-virus software automatically fixes the problem).

Access Security

All members of staff/councillors are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this policy.

The Parish Council has a secure firewall and anti-virus software in place. These prevent individuals from unauthorised access and to protect the Parish Council's network. The Parish Council also teach individuals about e-safety to ensure everyone is aware of how to protect the Parish Council's network and themselves.

Communications and Transfer.

You should be careful about maintaining confidentiality when speaking in public places.

You should make sure to mark confidential information 'confidential' and circulate this information only to those who need to know the information in the course of their work for the Parish Council.

Personal or confidential information should not be removed from the Parish Council without prior permission from the Clerk and Responsible Officer except where the removal is temporary and necessary. When such permission is given you must take all reasonable steps to ensure that the integrity of the information and the confidentiality are maintained.

You must ensure that the information is:

a) not transported in see-through or other un-secured bags or cases;
b) not read in public places (e.g. waiting rooms, cafes, trains, etc.); and
c) not left unattended or in any place where it is at risk (e.g.in car boots, cafes, etc.)

Reporting Security Breaches

All concerns, questions, suspected breaches, or known breaches shall be referred immediately to the Clerk and Responsible Officer. All members of staff/councillors have an obligation to report actual or potential data protection compliance failures.

When receiving a question or notification of a breach, the Clerk and Responsible Officer shall immediately assess the issue, including but not limited to, the level of risk associated with the issue, and shall take all steps necessary to respond to the issue.

Members of staff/councillors shall under no circumstances attempt to resolve an IT security breach on their own without first consulting the Clerk and Responsible Officer. Any attempt to resolve an IT security breach by a member of staff/councillors must be under the instruction of, and with the express permission of, the Clerk and Responsible Officer/Chair.

Missing or stolen paper records or mobile devices, computers or physical media containing personal or confidential information should be reported immediately to the Clerk and Responsible Officer.

All IT security breaches shall be fully documented.

Full details on how to notify of data breaches are set out in the Security Incident and Data Breach Notification Policy.

6. Information Sharing Policy

Deciding to share personal data

Personal data sharing is not an automatic assumption and there must be:-

- a clear objective or set of objectives as to what the sharing is meant to achieve
- a legal basis
- some form of active communication where the individual knowingly indicates consent
- A valid information sharing agreement in place unless exceptional circumstances apply.
-

Information sharing must only be done in adherence with the General Data Protection Regulation and Data Protection Act 2018 in line with the Information Commissioner's Data Sharing Code of Practice

Sharing information without an individual's knowledge is permitted for:-

- the prevention or detection of crime
- the apprehension or prosecution of offenders; or
- the assessment or collection of tax or duty

Process

All ISA's should be drafted using the Parish Council's standard Information Sharing Agreement Template (Appendix 1). The Clerk and Responsible Officer should be consulted when it is believed an ISA is required.

You must ensure when entering into any regular information sharing arrangements that an Information Sharing Agreement is in place and that it states a clear and lawful legal basis to allow the sharing to take place and it is agreed by all parties and approved by the Clerk and Responsible Officer.

All information sharing agreements must be regularly reviewed and will be stored centrally by the Parish Council and published on the Parish Council's website.

7. Security Incident and Data Breach Policy

Kings Hill Parish Council ('the Parish Council') is responsible for the protection of individuals about the processing of personal data and is legally required under the Directive 95/46/EC General Data Protection Regulation 2016/679 (GDPR) and the Data Protection Act 2018 to comply with these requirements.

Every care must be taken to protect information and to avoid a security incident, especially where the result is a data breach when personal information is lost or disclosed inappropriately to an unauthorised person. In the unlikely event of such a security incident it is vital that appropriate action is taken to minimise any associated risk. The Parish Council will investigate all security incidents classified as 'serious' using a set plan and follow a Breach Management Plan in the event of a data breach.

Obligations and responsibilities under the General Data Protection Regulation are not optional; they are mandatory. There can be harsh penalties, up to €20 million or 4% of global turnover for the preceding year (whichever is the greater) in relation to breaches of rights and obligations and up to €10 million or 2% of global turnover for the preceding year (whichever is the greater) imposed for non-compliance regarding Control and Mitigation.

All individuals permitted to access personal data in line with their work must agree to comply with this policy and agree to undertake any relevant training that may be appropriate.

Contact Officer: Georgina Jackson, Deputy Clerk

Date: 5th January 2021