Knights of St Columba

Data Protection & Privacy Policy

May 2018

This Policy sets out the Data Protection and Privacy Policy for the Knights of St. Columba (the Organisation's) strategic commitment to data protection. It is the policy of the Organisation to ensure that the Organisation treats personal information lawfully and correctly in order to:

- Maintain the trust and confidence of those with whom it does business
- Meet the Organisation's contractual, legal and regulatory obligations and in particular the protection of the rights of data subjects in respect of their personal data under EU Regulation 2016/679 the General Data Protection Regulation ("GDPR")

For the purposes of this Data Protection Policy "personal data" is any information relating to an identified or identifiable natural person (a "data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

This Policy sets the Organisation's obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by the Organisation, its employees, members, agents, contractors, or other parties working on behalf of the Organisation.

Data Protection shall be treated as an integral part of management activities and will be pursued in the same manner and with the same vigour as other management objectives.

This Policy is intended to ensure compliance with the GDPR.

Knights of St Columba

Data Protection & Privacy Policy

May 2018

Contents

The Rights of Data Subjects (Articles 15-22 GDPR)

I. The Organisation will observe and respect the rights applicable to data subjects in respect of data that we collect and manage on our own behalf as data controller.

II. Where we host and process personal data on behalf of a third-party data controller as part of the services offered or made available to our customers then, in the event that we are notified or informed by a data subject that they wish to exercise their rights under the GDPR, the Organisation shall promptly and without undue delay transmit or refer such request(s) to the data controller for action and shall advise the data subject of the referral and provide the name and contract details of the data controller.

III. Certain personal data is collected and managed by the Organisation on behalf of the data controller as part of a statutory/duty of care obligation owed to co-workers and/or the general public by the controller. In such cases the right to erasure (right to be forgotten) may be overridden by an obligation on the part of the data controller to comply with a legal obligation to which they are subject. In such circumstances the data controller will be justified in continuing to process the data despite such request for the duration of the obligation.

Lawfulness of Processing (Article 6 GDPR)

The Organisation before processing any personal data shall ensure that at least one of the following applies: -

a) the data subject has given consent to the processing of their personal data for one or more specific purposes;

b) the processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract with them;

c) the processing is necessary for compliance with a legal obligation to which the data controller is subject;

d) the processing is necessary to protect the vital interests of the data subject or of another natural person;

e) the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or

f) the processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third-party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data.

Data Processing Principles (Article 5 GDPR)

I. The Organisation shall procure:-

a) That it only collects, processes, and holds personal data for the specific purposes set out in this Policy (or for other purposes expressly permitted by the GDPR) and that data subjects are kept informed at all times of the purpose or purposes for which the Organisation uses their personal data.

b) That Personal data collected by the Organisation as data controller for our own processing or, if hosted or processed by the Organisation for and on behalf of third party data controllers, will be processed lawfully, fairly, and transparently, without adversely affecting the rights of data subjects.

c) That personal data will be collected and/or processed for specified, explicit, and legitimate purposes and will not be further processed in a manner that is incompatible with those purposes.

d) That it will only collect and process personal data for and to the extent necessary for the specific purpose or purposes about which data subjects have been informed (or will be informed) and as set out in this Data Protection Policy. The personal data will be adequate, relevant and limited to the purposes for which it was collected or provided.

e) The Organisation shall ensure that all personal data collected, processed, and held by it in its own right and for its own internal purposes is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject.

The accuracy of personal data shall be checked when it is collected and at 12-month intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate. In the case of personal data that is supplied to the Organisation by a third-party data controller or by an individual data subject for processing as part of the services provided to that data controller, the Organisation shall make available within the services suitable utilities, tools and functions to allow the data controller to meet their GDPR obligations in this respect.

Data Retention

I. The Organisation shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed. When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay. For more details of the Organisation's approach to data retention, including retention periods for specific personal data types held by the Organisation for internal use please request a copy of our Data Retention Policy. Contact details can be found in this document.

II. Personal data supplied by third party data controllers or collected from data subjects on behalf of such third parties as part and parcel of the services we provide will be retained for a period or periods to be determined by the data controller's own policies and obligations under GDPR. The Organisation will provide the data controller with the capability to edit, correct, archive and delete personal information relating to registered data subjects within their own secure account(s). The Organisation will only intervene in the management of personal data upon specific and explicit written instruction from the data controller.

Secure Processing (Article 32 GDPR)

The Organisation taking into account the state of the art, the costs of implementation and the scope and nature of the processing as well as the risk to the rights and freedoms of data subjects, shall take appropriate and commensurate steps to ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

Personal data will be encrypted for security purposes

Accountability and Record-Keeping (Article 30 GDPR)

I. The Organisation's Responsible Officer for Data Protection is an Appointed Member. Contact information is provided below.

Ray Pealing,
Knights of St Columba,
75 Hillington Road South,
Glasgow, Scotland. G52 2AE
Tel: 0141 883 5700 email: dpo@ksc.org.uk

II. The Responsible Officer with the support of the Supreme Knight and the Board of Directors shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Organisation's other data protection-related policies, and with the GDPR and other applicable data protection legislation.

III. The Organisation shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information according to the nature of the personal information and the reasons for its collection and processing:

a) the name and details of the Organisation, its Responsible Officer, and any applicable third-party data processors;

b) the purposes for which the Organisation collects, holds, and processes personal data;

c) details of the categories of personal data collected, held, and processed by the Organisation, and the categories of data subject to which that personal data relates;

d) details of any permitted transfers of personal data to other EEA countries including transfer mechanisms and security safeguards. Personal data collected in connection with the provision of services by the Organisation to its customers will not be transferred outside the EEA without specific written authority from the data controller and the appropriate Government agency;

e) details of how long personal data will be retained by the Organisation (please refer to the Organisation's Data Retention Policy); and

f) detailed descriptions of all technical and organisational measures taken by the Organisation to ensure the security of personal data.

Data Protection Impact Assessments (Article 35 GDPR)

I. The Organisation shall consider the implications for Data Protection for any and all new projects and/or new uses of personal data which involve the use of new technologies where the processing involved is likely to result in a high risk to the rights and freedoms of data subjects under the GDPR.

II. The Impact Assessment and Data Protection implications shall be included in the Organisation's formal Project Scope Document as a separate item

Keeping Data Subjects Informed (Articles 13 & 14 GDPR)

I. The Organisation shall provide the information set out below to every data subject:

a) Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and

b) Where personal data is obtained from a third-party data controller, the relevant data subjects will be informed of its purpose:

i. if the personal data is used to communicate with the data subject, when the first communication is made; or

ii. if the personal data is to be transferred to another party, before that transfer is made; or

iii. as soon as reasonably possible and in any event not more than one month after the personal data is obtained

II. The following information shall be provided in the form of a processing notice:

a) Details of the Organisation including, but not limited to, the identity of its Responsible Officer;

b) The purpose(s) for which the personal data is being collected and will be processed and the legal basis justifying that collection and processing;

c) Where applicable, the legitimate interests upon which the Organisation or the data controller is justifying its collection and processing of the personal data;

d) Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;

e) Where the personal data is to be transferred to one or more third parties, details of those parties;

f) Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the "EEA"), details of that transfer, including but not limited to the safeguards in place;

g) Details of data retention;

h) Details of the data subject's rights under the GDPR;

i) Details of the data subject's right to withdraw their consent to the Organisation's processing of their personal data at any time;

j) Details of the data subject's right to complain to the Information Commissioner's Office (the "supervisory authority" under the GDPR);

k) Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and

l) Details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

Data Subject Access (Article 15 GDPR)

I. Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which the Organisation holds about them, what it is doing with that personal data, and why.

II. Employees wishing to make a SAR should do so using a Subject Access Request, sending the request to the Organisation's Responsible Officer at dpo@ksc.org.uk The use of a form is not a mandatory requirement and the Organisation will respond to any written request from a data subject that amounts to a clear and unequivocal request to disclose this information.

III. Where the Organisation is acting as data processor for a third-party data controller, we shall pass the SAR to the controller and advise the data subject of this action and confirm the name of the data controller within 3 working days.

IV. Responses to SARs shall normally be made within one month of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

V. All SARs received shall be managed by the Organisation's Responsible Officer.

VI. The Organisation does not charge a fee for the handling of normal SARs. The Organisation reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

Rectification of Personal Data (Article 16 GDPR)

I. Data subjects have the right to require the Organisation acting as data controller to rectify any of their personal data that is inaccurate or incomplete.

II. The Organisation shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the Organisation of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

III. In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

IV. Where the Organisation is acting as data processor for a third-party data controller, we shall pass the request for rectification to the controller within three working days and advise the data subject of this action and confirm the name of the data controller. The Organisation has provided the data controller with the means to rectify personal data within their account and it the responsibility of the data controller to make such rectification under their service contract with the Organisation and to notify the data subject in accordance with Article 19 of the GDPR.

Erasure of Personal Data (Article 17 GDPR)

I. Data subjects have the right to request that the Organisation acting as a data controller erases the personal data it holds about them in the following circumstances:

a) it is no longer necessary for the Organisation to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;

b) the data subject wishes to withdraw their consent to the Organisation holding and processing their personal data;

c) the data subject objects to the Organisation holding and processing their personal data (and there is no overriding legitimate interest to allow the Organisation to continue doing so);

d) the personal data has been processed unlawfully;

e) the personal data needs to be erased in order for the Organisation to comply with a particular legal obligation.

Restriction of Personal Data Processing (Article 18 GDPR)

I. Data subjects may request that the Organisation ceases processing the personal data it holds about them. If a data subject makes such a request, the Organisation shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

II. In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

III. Where the Organisation is acting as data processor for a third-party data controller, we shall pass the request for restriction to the controller within three working days and advise the data subject of this action and confirm the name of the data controller. The Organisation has provided the data controller with the means to manage personal data within their account and it the responsibility of the data controller to take appropriate action in relation to such subject requests under their service contract with the Organisation and to notify the data subject in accordance with Article 19 of the GDPR.

Data Portability (Article 20 GDPR)

I. Where data subjects have given their consent to the Organisation to process their personal data in such a manner, or the processing is otherwise required for the performance of a contract between the Organisation and the data subject, data subjects have the right, under the GDPR, to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers).

II. To facilitate the right of data portability, the Organisation shall make available all applicable personal data to data subjects in the following format[s]: Excel or CSV .

III. Where technically feasible, if requested by a data subject, personal data shall be sent directly to the required data controller.

IV. All requests for copies of personal data shall be complied with within one month of the data subject's request. The period can be extended by up to two months in the case of complex or numerous requests. If such additional time is required, the data subject shall be informed.

V. Where the Organisation is acting as data processor for a third-party data controller, we will pass any subject request to receive personal data to the data controller within 3 working days. We will provide the data in the format(s) requested from the list in item II (above) upon written instructions for the same from the data controller.

Objections to Personal Data Processing (Article 21 GDPR)

I. Data subjects have the right to object to the Organisation acting as data controller processing their personal data based on legitimate interests, direct marketing (including profiling), and processing for scientific and/or historical research and statistics purposes.

II. Where a data subject objects to the Organisation processing their personal data based on its legitimate interests, the Organisation shall cease such processing immediately, unless it can be demonstrated that the Organisation's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

III. Where a data subject objects to the Organisation processing their personal data for direct marketing purposes, the Organisation shall cease such processing immediately.

Profiling (Article 22 GDPR)

1. The Organisation uses personal data for limited profiling purposes: -

   a) Where the Organisation is data controller, to manage customer accounts;

   b) Where the Organisation is acting as data processor in the provision of services to third-party data controllers.

2 When personal data is used for profiling purposes, the following shall apply:

   c) Appropriate mathematical or statistical procedures shall be used; and

   d) Technical and organisational measures shall be implemented to minimise the risk of errors.;

   and

   e) All personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling.

Personal Data Collected, Held, and Processed

The following personal data is collected, held, and processed by the Company (for details of data retention, please refer to the Company's Data Retention Policy):

DATA REFERENCE	TYPE OF DATA	PURPOSE OF DATA
Accounts Data Data Controller	• Organisation Name • Organisation Address • Contact Numbers • Telephone • Fax • Emails • Website • Product(s) / Services taken by Customer • Prices and Tariffs • Invoice Contact Emails Telephone • Orders Items Dates Product Types Quantities Values • Invoice / Credits Numbers (Incl. Dates and Amounts)	To manage and support the provision of services to members
CRM Systems Data Controller	• Client / Prospect Company Name Company Address • Group Company Name Number of Employees Telephone Website Fax Contact Details Emails Mobile Numbers Job Title / Office • Contact Preference • Estimated values • Driver Licence Check • Posts Notes (Free Text) • Actions & Dates (Free Text) • Linked Documents stored in Outlook (Emails, Texts, Scanned Contracts, etc.) • Contracts sent & returned • Opted into Marketing • Purchase Spends & history • Follow Up / Next Contract • Accounts information	Sales Order Processing, Membership Activities, Account Managements and Prospecting / Marketing Data

DATA REFERENCE	TYPE OF DATA	PURPOSE OF DATA
Outlook / Exchange	• Contact Names • Contact Addresses • Contact Telephones • Contact Email Addresses • Previous Correspondence • Diary & Meeting Dates	Communication and Management of correspondence
Personnel Records	• Names • Date of Birth • National Insurance Number • Start Date / End date • Salary • Job Title • DBS Checks • I D Checks • Document Images • Grey Fleet Data • Expenses • Training Records • Qualifications • CV (Copy) • Leave • Sickness • Contract of Employment • Confidentiality Agreement • Variation Agreements (if any) • Correspondence • Tax and PAYE Information • P11D Information • Disciplinary Records	Managing Employees
Members' Records	• Names • Address • Telephone/Mobile Numbers • Email Addresses • Facebook Accounts • Date of Birth • Marital Status • Membership Number • Council Number • Province Number • Initiation Date • Degree Date(s) • Meritorious Service Award • Silver Jubilee Award • Golden Jubilarian Award • Age • Under 21 • Over 75 • Columba Magazine Subscription • Lapsations / Resignation • Suspension	Managing Members

Youth and Young People

The Organisation undertakes various youth works including competitions and seminars. To comply with GDPR it refers to Article 5 of GDPR which is found on Page 4 of this Privacy Policy.

In addition to this, consent from a parent, guardian or responsible person or body, (for example a teacher and/or school), is required relating to a data subject of 12 years or under in Scotland, and 13 years or under in England and Wales.

Data Security - Transferring Personal Data and Communications

The Organisation shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data: -

a) All emails containing personal data must be encrypted and/or password protected to protect the content;

b) All emails containing personal data must be marked "confidential"; Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;

c) Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;

d) Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted;

e) Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using recorded delivery in a sealed envelope or parcel; and

f) All personal data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked "confidential".

Data Security – Storage

The Organisation shall ensure that the following measures are taken with respect to the storage of personal data:

a) All electronic copies of personal data should be stored securely using passwords and **industry standard** data encryption;

b) All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar;

c) All personal data stored electronically should be backed up daily with backups stored onsite **AND/OR** offsite. All backups should be encrypted using industry standard encryption;

d) No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to the company or otherwise without

the formal written approval of the Knights of St. Columba Data Protection Officer (Ray Pealing) and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary; and

e) No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Organisation where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the GDPR (which may include demonstrating to the Organisation that all suitable technical and organisational measures have been taken).

Data Security - Disposal

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed) it will be securely deleted and disposed of. For further information on the deletion and disposal of personal data, please refer to the Organisation's Data Retention Policy.

Data Security - Use of Personal Data

I. The Organisation shall ensure that the following measures are taken with respect to the use of personal data:

a) No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the Organisation requires access to any personal data that they do not already have access to, such access should be formally requested from the Responsible Officer (Ray Pealing);

b) No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Organisation or not, without the authorisation of the Responsible Officer (Ray Pealing);

c) Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time;

d) If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it; and

e) Where personal data held by the Organisation is used for any type of membership or marketing purposes, it shall be the responsibility of the Supreme Director for that Department to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS.

Where the Organisation is acting as data processor for and on behalf of a third-party data processor in the provision of services to that controller, personal data belonging to the data controller may not be used for any purpose or to any end that is inconsistent with the purpose for which it was originally provided or which is outside the terms of the contract under which the processor has agreed to provide the services to the controller.

Data Security - IT Security

I. The Organisation shall ensure that the following measures are taken with respect to IT and information security:

a) All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols.

b) Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Organisation, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;

c) All software (including, but not limited to, applications and operating systems) shall be kept up-to-date. The Organisation's IT staff shall be responsible for installing any and all security-related updates as soon as reasonably and practically possible unless there are valid technical reasons not to do so; and

d) No software may be installed on any Organisation-owned computer or device without the prior approval of the Knights of St Columba Data Protection Officer.

e) All data held in IT systems shall be encrypted for security purposes using industry standard encryption software.

II. Where the Organisation is acting as data processor in the provision of services to the data controller, access to personal data stored in the controller's account shall be restricted to nominated personnel only. Those personnel shall have their access controlled by user name and passwords that shall meet minimum standards and will change regularly. Access shall be recorded in log files.

Organisational Measures

The Organisation shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

All employees, members, agents, contractors, or other parties working on behalf of the Organisation shall be made fully aware of both their individual responsibilities and the Organisation’s responsibilities under the GDPR and under this Policy, and shall be provided with a copy of this Policy;

a) Only employees, agents, sub-contractors, or other parties working on behalf of the Organisation that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Organisation;

b) All employees, agents, contractors, or other parties working on behalf of the Organisation handling personal data will be appropriately trained to do so;

c) All employees, agents, contractors, or other parties working on behalf of the Organisation handling personal data will be appropriately supervised;

d) All employees, agents, contractors, or other parties working on behalf of the Organisation handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;

e) Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;

f) All personal data held by the Company shall be reviewed periodically, as set out in the Organisation's Data Retention Policy;

g) The performance of those employees, agents, contractors, or other parties working on behalf of the Organisation handling personal data shall be regularly evaluated and reviewed;

h) All employees, agents, contractors, or other parties working on behalf of the Organisation handling personal data will be bound to do so in accordance with the principles of the GDPR and this Policy by contract;

i) All agents, contractors, or other parties working on behalf of the Organisation handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Organisation arising out of this Policy and the GDPR; and

j) Where any agent, contractor or other party working on behalf of the Organisation handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Organisation against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

Transferring Personal Data to a Country Outside the EEA

I. The Organisation will not transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA.

Where the Organisation provides services to third-party data controllers, it is a requirement in the contract for the provision of such services that the data controller does not transfer or allow access to driver record data sourced from the DVLA from outside the EEA without first obtaining written approval from the DVLA. The DVLA will not provide such approval unless it is satisfied that there are appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the GDPR); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority.

Data Breach Notification

I. All personal data breaches must be reported immediately to the Organisation's Responsible Officer and the Licence Check Security Officer.

II. If a personal data breach occurs in respect of data for which the Organisation is the data controller and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Responsible Officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

III. In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 29.2) to the rights and freedoms of data subjects, the Responsible Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

IV. Data breach notifications shall include the following information:

a) The categories and approximate number of data subjects concerned;

b) The categories and approximate number of personal data records concerned;

c) The name and contact details of the Organisation's data protection officer (or other contact point where more information can be obtained);

d) The likely consequences of the breach;

e) Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

Where the Organisation is acting as data processor for a third-party data controller, the obligations in I - IV above shall apply, but notification shall be to the data controller rather than to the data subjects directly.

Implementation of Policy

This Policy shall be deemed effective as of 25/05/2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by the Directors of the Knights of St Columba.

Policy Updates

Page 13 - Reference to Youth and Young People added - 25th September 2018.
Page 13 - Reference to Youth and Young People amended - 27th September 2018.
Page 3 – Accountability and Record-Keeping (Article 30 GDPR) – Name of Data Protection Officer amended – 25th April 2019
Page 12 – Data Security – Use of Personal Data – Name of Responsible Officer amended – 25th April 2019