Data Protection policy

Introduction

The purpose of this policy is to ensure that you are aware that everyone has a responsibility to comply with the principles and legal conditions provided by the data protection legislation, including the GDPR, and failure to meet those responsibilities are likely to lead to serious consequences. , which could include internal disciplinary procedures, criminal proceedings or a fine for King's which could theoretically be up to £17.5 million! However frustrating this policy seems at times we need to take it very seriously and the consequences demonstrate this.

If you are in any doubt about what you can or cannot disclose and to whom, do not disclose the personal information until you have sought further advice from King's Data Representatives, currently Ed Beckingham and Dave Pull (data@kings-norwich.com).

Throughout this document we have used the term King's referring to our various legal and trading names. Your employment is with King's Church Centre Norwich (KCCN), which is usually referred to as King's Community Church. The trading arm of King's is King's Church Centre Facilities Norwich and usually referred to as The King's Centre.

Definitions

Data Subject: a living individual.
Data Controller: the person or organisation that determines the means and the purpose of processing the personal data.
Data Protection Legislation: includes (i) the Data Protection Act 2018, (ii) the General Data Protection Regulation ((EU) 2016/679) **(GDPR)** and any national implementing laws, regulations and secondary legislation, for so long as the GDPR is effective in the UK, and (iii) any successor and supplemental legislation to the Data Protection Act 1998, the Data Protection Act 2018, the GDPR and the E-Privacy Directive 2002, revised in 2009 (and its proposed replacement), once it becomes law.
Personal data: is any information that identifies a living individual (data subject) either directly or indirectly. This also includes special categories of personal data. Personal data does not include data which is entirely anonymous or the identity has been permanently removed, making it impossible to link back to the data subject.
Processing: is any activity relating to personal data which can include collecting, recording, storing, amending, disclosing, transferring, retrieving, using or destruction.
Special categories of personal data: this includes any personal data which reveals a data subject's: ethnic origin, political opinions, religious and philosophical beliefs, trade union membership, genetic, biometric or health data, sex life and sexual orientation.
Criminal records data: means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

What are the GDPR principles?

We are a data controller. This means that we are required by law to ensure that everyone who processes personal data and special categories of personal data during the course of their work with us, does so in accordance with the data protection legislation.. In brief, this means that:

- Personal data must be processed in a lawful, fair and transparent way.

- The purpose for which the personal information is collected must be specific, explicit and legitimate.
- The collected personal data must be adequate and relevant to meet the identified purpose.
- The information must be accurate and kept up to date.
- The personal data should not be kept in a form which permits identification of a data subject for longer than is necessary for the purposes for which it is used.
- The personal data must be kept confidential and secure and only processed by authorised personnel.
- The data subject must be permitted to exercise their rights in relation to their personal data.

King's and all our employees and volunteers must comply with these principles and rules at all times, in their information-handling practices. We are committed to ensuring that these principles and rules are followed, as we take the security and protection of data very seriously.

You must inform us immediately if you become aware that any of these principles or rules have been breached or are likely to be breached.

WHAT ARE THE LAWFUL REASONS UNDER WHICH WE WOULD EXPECT YOU TO PROCESS PERSONAL DATA?

Whilst carrying out your work activities, you are likely to process personal data. King's will only expect you to process personal data where the business has a lawful basis (or bases) to process that information. The lawful basis may be any one of the following reasons or a combination of:

a) Consent has been obtained by the data subject to process their personal data for specified purposes.
b) Where we need to perform the contract, we have entered into with the data subject, either for employment, volunteering or commercial purposes.
c) Where we need to comply with a legal obligation.
d) Where it is necessary for our legitimate interests (or those of a third party), and the interests and fundamental rights of the data subject do not override those interests.

There are other rare occasions where you may need to process the data subject's personal information, these include:

e) Where we need to protect the data subject's interests (or someone else's interests).
f) Where it is needed in the public interest [or for official purposes].

We keep a list of the legal basis for each activity on our data mapping sheet, so check with the Data Representative for more information.

PRIVACY NOTICES

Personal data must be processed in a lawful, fair and transparent way.

Before you begin collecting or processing personal data directly from a data subject, you must ensure that an appropriate privacy notice has been issued to the data subject.

Check that you are using an up to date and relevant version of our privacy notice and it is being used in accordance with the King's guidelines.

➔ Purpose Limitation
  - The purpose for which the personal information is collected must be specific, explicit and legitimate. If it becomes necessary to use the information for a reason other than the reason which you have previously identified, you must usually stop processing that information.

➔ Adequate and Relevant
  - The collected personal data must be adequate and relevant to meet the identified purpose.
  - You must only process personal data where you have been authorised to do so because it relates to your work or you have been delegated temporary responsibility to process the information. You must not collect, store or use unnecessary personal data and you must ensure that personal data is deleted, erased or removed within King's

retention guidelines. You must not process or use personal data for non-work related purposes.

➔ Accurate and kept up to date.
- You must keep the information accurate and kept up to date, checking regularly (e,g, annually) with the data subject.

➔ Kept for longer than is necessary
- The personal data should not be kept in a form which permits identification of a data subject for longer than is necessary for the purposes for which it is used.
- Different categories of personal data will be retained for different periods of time, depending on legal, operational and financial requirements. We must destroy any data we do not need to hold for a particular period of time, in accordance with its retention of data policy. Speak to the Data Representative if you are unsure about when this is.

➔ Kept confidential and secure
- The personal data must be kept confidential and secure and only processed by authorised personnel. To achieve this you must follow these steps:
- King's has in place appropriate technical and organisational measures to protect against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of, or damage to, data. These procedures must always be adhered to, and not overridden or ignored.
- Ensure that any personal data which you hold is kept securely, either in a locked filing cabinet or, if it is computerised: it is password protected so that it is protected from unintended destruction or change and is not seen by unauthorised persons.
- Do not write down (in electronic or hard copy form) opinions or facts concerning a data subject which would be inappropriate to share with that data subject.
- Do not remove personal information from the workplace with the intention of processing it elsewhere, unless this is necessary to enable you to carry out your job duties and has been authorised by your line manager. If authorised to, continue to observe the terms of this policy and the data protection legislation, in particular: in matters of data security.
- Ensure that hard copy personal information is disposed of securely.
- Manual personnel files and data subject files are confidential and are stored in a locked filing cabinet. Only the Centre Manager is authorised to have access to these files. These will not be removed from their normal place of storage without good reason.
- Data held on computers are stored confidentially by means of password protection.
- King's has network back-up procedures to ensure that data on computers cannot be accidentally lost or destroyed. More information on King's security procedures can be obtained by contacting the Data Representative.

➔ Transfer to another country
- Transfer of personal data to countries or organisations outside of the EEA should only take place if appropriate measures are in place to protect the security of that data. We do not do this as standard and so this shouldn't be done without discussion with the Data Representative and the GDPR team.

I.T. Protocols

King's uses 3 main systems for managing personal information. Do not use any other systems without prior permission from the GDPR team.

1. The server and Microsoft Office applications are used for the storage of long term information. This is secured by password protection, firewall, antivirus software and security monitoring software on the server and individual computers.
2. Google Mail, Drive and the Google Workspace is used for the short term transfer of data along with more flexible working and sharing of documents. All Google Drive documents should be stored under the ownership of data@kings-norwich.com for the purposes of data subject requests and access should be removed to documents once it is no longer required.
3. Churchsuite is King's contact management system and should be the only way to manage contact data for the whole church. Serious consideration should be given to the export of any data from Churchsuite, either to any of the platforms above or in printed form. Linda Howes and the King's Churchsuite team will be happy to assist you to get information out as you require it - e.g. for reports, registers or team management, so that you don't need to export it to other systems.

4. Additional systems for using personal data are used by King's in very specific circumstances. These are Sage (accounts), Quickbooks and yourpayroll.co.uk (Payroll), Mailchimp (Newsletters), Timetastic (Leave management).

Netmatters ares our IT support providers and ensure that data is protected at all times. Their policy can be found at https://www.netmatters.co.uk/privacy-policy

Links to other security policies can be found below:

- Churchsuite https://churchsuite.com/security/
- Google https://policies.google.com/privacy?hl=en-US
- Microsoft https://www.microsoft.com/en-us/corporate-responsibility/privacy
- Quickbooks https://security.intuit.com/
- Sage https://www.sage.com/en-gb/legal/status/governance/
- Mailchimp https://mailchimp.com/about/security/
- Timetastic https://help.timetastic.co.uk/hc/en-us/articles/213787949-Timetastic-data-security
- yourpayroll.co.uk https://www.yourpayroll.org.uk/your-data
- Peoples Pension https://thepeoplespension.co.uk/privacy/

The data subject rights

The data subject must be permitted to exercise their rights in relation to their personal data.

Under the GDPR, subject to certain legal limitations, data subjects have available a number of legal rights regarding how their personal data is processed. At any time a data subject can request that King's should take any of the following actions, subject to certain legal limitations, with regard to their personal data:

- Allow access to the personal data
- Request corrections to be made to the data
- Request erasure of the data
- Object to the processing of the data
- Request that processing restrictions be put in place
- Request a transfer of personal data
- Object to automated decision making
- Notify the data subject of a data security breach

There are different rules and timeframes that apply to each of these rights. You must follow King's data Subject Access Request Procedure, which details how to deal with requests. Contact the Data Representative to start this process and the GDPR team will take over from there.

Categories of information

During the course of your employment you may be required to process personal data which falls into different categories: general personal data and special categories of personal data. All data should be processed in accordance with the privacy notice and in a confidential manner at all times. However, where that data is classed as a special category, extra care should be taken to ensure the privacy and security of that data. This means that you should maintain a high level of security and you should only share this data with those who are also authorised to process that data.

We may also require you to process special categories of information in connection with members, customers and other third parties.

You may be asked to process information in relation to criminal convictions. This should be processed with the highest degree of confidentiality and in accordance with any data protection legislation and privacy notices that are in force.

If you are unsure about how you should process general personal data or special categories of personal data, you must contact the Data Representative.

When will you need to seek consent?

In limited circumstances during your work you may need consent from a data subject in order to process personal data or special categories of data. You will be provided with training and details of which circumstances consent is needed and the type of consent that should be sought. However, in limited circumstances, you may find it necessary to request a data subject to provide written consent to allow the processing of special categories of personal data. For example, in an employment context you should request the data subject's written consent to instruct a medical practitioner to prepare a medical report. If it becomes necessary to request consent to process special categories of personal data, you must provide the data subject with details of the information that will be required and why it is needed, so that they can make an informed decision as to whether they wish to provide consent.

You must not compel a data subject to provide written consent. Giving consent will always be a decision made by freewill and choice and is not a contractual condition. Consent can be withdrawn at any time without any reason provided. You must not subject a data subject to a sanction or detriment as a consequence of withdrawing consent. This would be viewed a serious disciplinary issue.

Exemptions

In limited circumstances there are certain categories of personal data which are exempt from the GDPR regime; for example: in relation to employment:

- Confidential references that are given, but not those received by King's from third parties. Only designated line managers can give King's references. Confidential references will not be provided unless King's is sure this is the employee's wish.
- Management forecasts and management planning (including documents setting out management plans for an employee's future development and progress).
- Data which is required by law to be publicly available.
- Documents subject to legal professional privilege.

Action to be taken in the event of a personal data breach

A personal data breach will arise whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on a data subject.

In the event of a security incident or breach, do not try to handle this yourself. You must immediately informing the Data Representative so that steps can be taken to:

- Contain the breach;
- Assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen; and
- To limit the scope of the breach by taking steps to mitigate the effects of the breach.

The Data Representative will determine within 72 hours the seriousness of the breach, and if the Information Commissioner's Office (ICO) and/ or data subjects need to be notified of the breach.

Record keeping

As we have fewer than 250 employees, we only need to document processing activities that:

- are not occasional; or
- could result in a risk to the rights and freedoms of individuals; or
- involve the processing of special categories of data, or criminal conviction and offence data

Training

All employees that handle personal information of individuals must have a basic understanding of the data protection legislation, including the GDPR. Staff with duties, such as: computer and internet security, marketing and database management, may need specialist training to make them aware of particular data protection requirements in their work area.

We will provide you with continuous training and updates on how to process personal data in a secure and confidential manner, and in accordance with the spirit of the data protection legislation, including

the GDPR. You will be required to attend all training, and to keep yourself informed and aware of any changes made to privacy notices, consent procedures and any other policies and procedures associated with our internal processing of personal data.

You must regularly review all your data processing activities and ensure that you are acting in accordance with the most current best practice and legal obligations in relation to data security and confidentiality.

Sharing personal data

We may only share personal data internally as is necessary. You must always ensure that personal data is only shared with authorised persons and is shared in accordance with the purposes stated in any privacy notice or consents. Extra care and security must be taken when sharing special categories of data or transferring data outside of King's to a third party.

Direct Marketing

We are subject to specific rules under the GDPR in relation to marketing our services. Data subjects have the right to object to direct marketing and we must ensure that data subjects are given this option at first point of contact. When a data subject exercises their right to object to marketing, you must immediately remove them from your mailing lists, keep a record of their objection and stop sending further communications.

Complaints

If you believe that this policy has been breached by a colleague or to exercise all relevant rights, queries or complaints, please in the first instance contact our data representatives or your line manager.

Compliance with GDPR is everyone's responsibility.

By signing this policy, you confirm that you have read and understood the content of this policy, and that you agree to adhere to the content, and that you understand that breach of any aspect of this policy may lead to serious disciplinary action.

Signed by name of employee/ volunteer: ……..

Print name: ……

Date: …….