**WORK PLACE CHAPLAINCY SCOTLAND**

**Listening & caring - in confidence**

**DATA PROTECTION POLICY**

**1 Purpose and objectives**

This policy forms part of WPCS’s commitment to the safeguarding of personal data processed by its staff, volunteers, trustees, contractors and external contacts . Its objectives are:

* To help all parties recognise personal data
* To help them understand their rights and obligations with respect to personal data.

**2 Introduction**

WPCS processes the personal data of living individuals such as its staff, volunteers, contractors, partners and customers. This processing is regulated by the Data Protection Act 1998 (DPA) and is held under GDPR legislation from 25 May 2018. The UK’s regulator for the DPA is the Information Commissioner’s Office. This Policy has been updated under GDPR legislation to include the Privacy Notice found in Annex B.

It is the duty of data controllers such as WPCS to comply with the data protection principles (see the Annex to this Policy) with respect to personal data. This policy describes how WPCS will discharge its duties in order to ensure continuing compliance with the DPA in general, GDPR legislation, and the data protection principles and rights of data subjects in particular. The principles are listed in Annex A.

**3 Scope**

The policy applies to all staff, volunteers, trustees, contractors and contacts of WPCS. It relates to their use of any WPCS-owned facilities (and those leased by or rented or on loan to WPCS), centrally managed or otherwise; to all private systems (whether owned, leased, rented or on loan) when connected to WPCS; to all WPCS-owned or licensed data and programs (wherever stored); and to all data and programs provided to WPCS by sponsors or external agencies (wherever stored). The policy also relates to paper files and records created for the purposes of WPCS business.

**4 Definitions**

***Personal Data [1]***

‘”Personal data” means data which relates to a living individual who can be identified:

(a) from those data, or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual”

***Sensitive personal data [2]***

Information about:

* the racial or ethnic origin of data subjects
* their political opinions
* their religious beliefs or other beliefs of a similar nature
* whether they are members of a trade union
* their physical or mental health or condition
* their sexual life
* the commission or alleged commission by them of any offence, and any proceedings for such offences.

Although the DPA does not define ‘health’, the term should be understood broadly, to include preventative medicine, medical diagnosis, DNA sequences, medical research, provision of care and treatment and the management of healthcare services.

Personal demographic data, such as personal addresses and financial data (including salaries) are not sensitive personal data, but should be treated with similar care.

***Manual Personal Data***

Personal data recorded as part of a relevant filing system in paper or other non-electronic format.

***Processing [3]***

Obtaining, recording or holding personal data. This includes organisation, adaptation or alteration; retrieval, consultation or use; disclosure; and alignment, combination, blocking, erasure or destruction.

***Relevant Filing System [3]***

Manual personal data structured by reference to individuals in such a way that information relating to a particular individual is readily accessible.

***Data Holding***

A collection of one or more data sets or files that are being processed for permitted purposes under the direction of a clearly identified member of WPCS staff - the Data Owner.

***Data Controller***

As the organisation which determines the purposes of the processing, WPCS is the Data Controller for the personal data that it manages.

***Data Protection Officer***

The WPCS member of staff with lead responsibility for WPCS’s compliance with the DPA and GDPR, is currently the Secretary to the Board of Trustees.

***Data Owner***

The WPCS member of staff with lead responsibility for permitting and managing the retention and processing of a data holding for which WPCS is the Data Controller. Data Owners may delegate responsibility for personal data elements to the Data Custodian.

***Data Custodian***

The WPCS Administration Coordinator is responsible for the collection, creation, modification and deletion of specified personal data element(s).

***System Custodian***

The Chief Executive Officer has responsibility and authority to implement the Date Protection Policy, Data Privacy Policy, Data Security Policy, and supporting policies in respect of a WPCS-wide system, to ensure that the security measures adopted for systems under his/her control meet the requirements of these policies and to carry out the duties as set out in the associated Codes of Practice. Some duties may be delegated, to named persons whose particular duties are set out in writing, although the Custodian retains overall responsibility for the security of that system.

***Data Subject [4]***

A living individual who is the subject of personal data.

***Data Processor [4]***

Any third party (other than WPCS staff and volunteers) who processes personal data on behalf of and on the instructions of the Data Controller.

**5 Roles and responsibilities**

***Data Protection Officer***

The Data Protection Officer has primary responsibility for WPCS’s compliance with the DPA. This comprises:

* maintaining WPCS’s notification with the Information Commissioner’s Office
* ensuring completion of the Annual Survey of Personal Data Holdings
* handling subject access requests and requests from third parties for personal data
* promoting and maintaining awareness of the DPA and regulations, including training
* investigating losses and unauthorised disclosures of personal data.

The DPO is WPCS’s main contact for the Information Commissioner’s Office.

***Regional Organisers***

Regional Organisers are responsible for ensuring their staff and volunteers understand the role of the data protection principles in their day-to-day work, through induction, training and performance monitoring.

***Data Owner ( Individual Staff/Volunteers)***

Data Owners are responsible for:

* establishing and monitoring measures, in accordance with this policy and the information security policy, to protect any holdings of personal data for which they are responsible
* ensuring that those holdings are registered as part of the annual survey of personal data holdings
* ensuring that any transfer of personal data to third parties is authorised, lawful and uses appropriate safe transport mechanisms such as encryption.
* authorising the downloading of electronic personal data on to portable devices or the removal of manual personal data from WPCS premises
* informing their departmental Data Protection Coordinator when new holdings of personal data are established or when the purposes of processing change.

***Data Custodian***

The Data Custodians should ensure that their processing of personal data is compatible with the data protection principles, including the security and integrity of data sets.

***Data Processors***

Data processors have a contractual responsibility to act only on WPCS’s instructions and to ensure that their processing of personal data provided by WPCS is carried out in compliance with this policy and in accordance with the eight data protection principles. There should be a written agreement with data processors which adequately addresses these responsibilities.

***Staff and volunteers***

All staff and volunteers are responsible for:

* ensuring that their processing of personal data, including research data, in all formats (e.g. electronic, microfiche, paper, etc.) is compatible with the data protection principles
* raising any concerns in respect of the processing of personal data with the Data Protection Officer
* promptly passing on to the Data Protection Officer all subject access requests and requests from third parties for personal data
* reporting losses or unauthorised disclosures of personal data to the Data Protection Coordinator.
* ensuring that the personal data they provide about themselves is up to date in order that WPCS can continue to comply with the fourth data protection principle.

**6 Security of personal data**

All staff and volunteers processing personal data should ensure that the data are secure: appropriate measures must be taken to prevent unauthorised access, disclosure and loss. Staff whose work includes responsibility for supervision of volunteers have a duty to ensure that volunteers observe the eight principles of the Act.

It is rarely necessary to store electronic personal data on portable devices such as laptops, USB flash drives, portable hard drives, CDs, DVDs, or any computer not owned by WPCS. Similarly, manual personal data should not be regularly removed from WPCS premises.

Manual personal data and portable electronic devices should be stored in locked units, and should not be left on desks overnight or in view of third parties.

In order to comply with the fifth data protection principle personal data should be securely destroyed when no longer required, with consideration for the format of the data.

Personal data must not be disclosed unlawfully to any third party. Transfers of personal data to third parties must be authorised in writing by the data owner and protected by adequate contractual provisions or data processor agreements, must agree with WPCS’s notification and must use safe transport mechanisms.

All losses of personal data must be reported to the Data Protection Coordinator and the Data Protection Officer. Negligent loss or unauthorised disclosure of personal data, or failure to report such events, may be treated as a disciplinary matter and could be considered gross misconduct.

**7 Publication of staff information**

WPCS will make public as much corporate information as possible. The following types of personal information will usually be published:

* Names of members of the Board of Trustees and their appointees
* Lists and directories of staff, including name, mobile telephone number and WPCS email address
* Research and training information

However, there are circumstances in which, for security and other reasons, agreed subsets of the above data about WPCS staff will not be published.

**8 Access to personal data**

***8.1 Subject access rights***

Data subjects have a right of access to their personal data, including some unstructured manual personal data. Subject access requests must be made in writing, and sent to the Data Protection Officer. Data subjects must prove their identity.

Copies will be provided in permanent form promptly and in any event within 40 days.

Some personal data are exempt from the right of subject access, including confidential references provided by WPCS and some research data.

WPCS does not charge a fee for subject access requests.

Although the DPA applies only to living individuals, data about deceased persons who at the time of processing would be under 100 years old should be treated as personal data, unless the information is the subject of a valid request under Freedom of Information legislation.

***8.2 Third party access***

In certain circumstances the DPA provides for disclosure of personal data, without the consent of the data subject, to certain organisations. Requests for such disclosures from third parties, such as the police, UK Border Agency, local authorities or sponsors, should be made in writing and handled by the Data Protection Officer. This will ensure the validity of the request and any warrants or orders of court can be checked. Staff disclosing personal data may not be protected by an invalid warrant.

**9 Status**

WPCS's Data Protection policy has been approved by WPCS's Board of Trustees. It is a condition of employment that employees will abide by the regulations and policies made by WPCS. Likewise, these are an integral part of the regulations for volunteers.

**ANNEX A**

**THE DATA PROTECTION PRINCIPLES**

It is the duty of data controllers and data processors to comply with all the data protection principles. These are set out in Schedule 1 of the Data Protection Act 1998, from which the following extract is taken:

1 Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

(a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2 Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3 Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4 Personal data shall be accurate and, where necessary, kept up to date.

5 Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6 Personal data shall be processed in accordance with the rights of data subjects under this Act.

7 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8 Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

**ANNEX B**

**Privacy Notice**

**Your personal data – what is it?**

Personal data relates to a living individual who can be identified from that data. Identification can be by the information alone or in conjunction with any other information in the data controller’s possession or likely to come into such possession. The processing of personal data is governed by the General Data Protection Regulation (the GDPR).

**Who are we?**

Work Place Chaplaincy Scotland (WPCS) is Scottish Charity (SC041857) and a Company Limited by Guarantee (SC387207). WPCS is committed to protecting and respecting your privacy. For any personal data you provide for the purpose of your WPCS employment or voluntary service, WPCS is the “Data Controller” and is responsible for storing and otherwise processing that data in a fair, lawful, secure and transparent way. We will only collect data that is required by legitimate interest for the purpose of administering your employment, voluntary service with us, or enquiries with us.

**How do we process your personal data?**

WPCS complies with its obligations under the GDPR by keeping personal data up to date; by storing and destroying it securely; by not collecting or retaining excessive amounts of data; by protecting personal data from loss, misuse, unauthorised access and disclosure and by ensuring that appropriate technical measures are in place to protect personal data.

**What personal data we hold on you and why**

We use your personal data for the following purposes: -

• To enable us to provide chaplaincy services for the benefit of the public as specified in our constitution;

• To fundraise and promote the interests of the charity;

• To manage our employees and volunteers;

• To maintain our own accounts and records (including the processing of donations and gift aid applications);

• To inform you of news, events and activities of the charity.

You may give us information about yourself by filling in an application form, or by corresponding with us by phone, e-mail or otherwise. Your information may fall under one of the following categories:

Employed Staff

Our legal basis for holding your information is as a “Legitimate Interest” in processing your employment with us - we will hold your title, name, date of birth, address, e-mail address, phone number, NI insurance number, and bank account detail. To care for the health and wellbeing of our staff, we will also ask for relevant health information, which is classed as special category personal data. In circumstances where you will work specifically with children or vulnerable adults, we are required under “Legal Obligation” to hold PVG status information under Disclosure Scotland legislation.

Volunteer

Our legal basis for holding your information is as a “Legitimate Interest” in administering your induction, training and voluntary service with us - we will hold your title, name, address, e-mail address, phone number, and bank account detail (if appropriate in the processing of any expense claim as approved by your Regional Organiser). In circumstances where you will work specifically with children or vulnerable adults, we are required under legal obligation to hold PVG status information under Disclosure Scotland legislation.

Trustee

Our legal basis for holding your information is as a “Legitimate Interest” in administering business conducted by the Board of Trustees - we will hold your title, name, email address and phone number. Additional for Trustees with bank authorisation, we will hold – and share with Unity Trust Bank plc – your bank application information. If you have made a declaration of interest, we will also hold the information you have disclosed to us on this form.

Contractor

Our legal basis for holding your information is as a “Legitimate Interest” in conducting our business with you – we will hold your contact name(s), address, email address, phone number and any other information required in order to conduct our mutual business with you, eg bank detail for invoicing purposes.

External Individual / External organisation contact

Our legal basis for holding your information is as a “Legitimate Interest” in administering your enquiry/s with us or in order to further our enquiry with you – we will hold your contact name, email address and phone number for as long as is necessary to retain contact with you whilst you wish to do so. You have the right to request your data be deleted from our systems at any time, and may do so by contacting: info@wpcscotland.co.uk.

**Who do we share information with?**

We will never sell your personal information. Your personal data will be treated as strictly confidential and will only be shared with third parties in order to meet statutory and legislative obligations.

**Third-party contractors:**

Mailings

To receive our regular newsletter, we will rely on the lawful basis of “Consent”. This means that we will record how and when you have signed up to receive this mailing. ‘Mailchimp’ is a “Third-Party Processor” of your data for the sole purpose of our newsletter mailing. Mailchimp is certified to the EU-U.S. Privacy Shield Framework and the Swiss-U.S Privacy Shield Framework. WPCS has obtained appropriate consent via our Mailchimp account, and can legally transfer contact data from the EU to MailChimp in the U.S. Mailchimp’s Private Policy can be accessed using this link: [Mailchimp Privacy Policy](https://mailchimp.com/legal/privacy/?mc_cid=e8a2ef89b4&mc_eid=e4f17dc2a9).

Financial Data

Whitelaw Wells – payroll provider to WPCS - is a “Third Party Processor” of full time paid staff data - data held by Whitelaw Wells under lawful basis for the “Legitimate Interest” in processing payroll: title, name, date of birth, address, e-mail address, phone number, NI insurance number, and bank account detail. Whitelaw Wells – Independent Examiner for WPCS – is a “Third Party Processor” of WPCS bookkeeping records - which will hold contact and bank detail (for invoicing purposes) of all WPCS suppliers and contractors - for the “Legitimate Interest” in conducting an annual audit or Independent Examination of WPCS accounts. To contact Whitelaw Wells, you can use this link: [Contact Whitelaw Wells](http://www.whitelawwells.co.uk/contactus/).

IT

Flonix Limited is a “Third-Party Processor” of IT data for support services to WPCS by “Legitimate Interest” in maintaining a communication and data storage system for WPCS. Flonix have set up Microsoft Office 365 for this purpose. To contact Flonix and to access their Privacy Notice you can use this link: [Contact Flonix](http://www.flonix.co.uk/contact/).

**Where do we process and store your information?**

The personal information collected by WPCS will be held in electronic and/or physical format on secured systems within the European Economic Area. We will not knowingly transfer your personal information outside of the European Economic Area. We only store physical copies of documents containing your personal information in our locked filing cabinet. Information that we store electronically is retained on Microsoft 365’s OneDrive, which is provided to us by Flonix IT services and managed by WPCS. You can access Microsoft’s privacy policy using this link: [Office 365 Privacy.](https://products.office.com/en-au/business/office-365-trust-center-privacy)

Details regarding how we store and manage data can be found in at: [Data Storage & Security Policy](WPCS%20Data%20Storage%20and%20Security%20Policy.docx)

**How do we protect your information?**

The security of your data is important to us, but remember that no method of transmission over the Internet, or method of electronic storage is 100% secure. While we strive to use commercially acceptable means to protect your Personal Data, we cannot guarantee its absolute security.

Further information about security and backup can be found at: [Data Backup Policy](WPCS%20Data%20Backup%20Policy.docx)

**Retention of Data – how long will we keep your data?**

In general we will retain personal data indefinitely unless notified by the data subject that they no longer wish us to hold or use their data for the purposes originally specified. Data will be securely deleted on receipt of any such notification.

Specifically, we retain gift aid declarations and associated paperwork for up to 6 years after the financial year (to 31 March) to which they relate, and information relating to staff and volunteer roles for up to 6 years after the role has ceased.

We will retain and use your Personal Data to the extent necessary to comply with our legal obligations (for example, if we are required to retain your data to comply with applicable laws), resolve disputes, and enforce our legal agreements and policies. Further information about retention can be found at: [Data Retention Policy.](WPCS%20Data%20Retention%20Policy.docx)

**Disclosure of Data**

Under certain circumstances, WPCS may be required to disclose your Personal Data if required to do so by law, or in response to valid requests by public authorities (e.g. a court or a government agency).

WPCS may disclose your Personal Data in the good faith belief that such action is necessary to:

* To comply with a legal obligation
* To protect and defend the rights or property of WPCS
* To prevent or investigate possible wrongdoing in connection with the Charity
* To protect the personal safety of users of the Service or the public
* To protect against legal liability.

**Your Rights**

Unless subject to an exemption under the GDPR, you have the following rights with respect to your personal data:

• The right to request a copy of your personal data which WPCS holds about you;

• The right to request that WPCS corrects any personal data if it is found to be inaccurate or out of date;

• The right to request your personal data is erased where it is no longer necessary for WPCS to retain such data;

• The right to withdraw your consent to the processing at any time;

• The right to request that the data controller provide the data subject with his/her personal data and where possible, to transmit that data directly to another data controller, (known as the right to data portability), (where applicable) [Only applies where the processing is based on consent or is necessary for the performance of a contract with the data subject and in either case the data controller processes the data by automated means];

• The right, where there is a dispute in relation to the accuracy or processing of your personal data, to request a restriction is placed on further processing;

• The right to object to the processing of personal data, (where applicable) [Only applies where processing is based on legitimate interests (or the performance of a task in the public interest/exercise of official authority); direct marketing and processing for the purposes of scientific/historical research and statistics];

• The right to lodge a complaint with the Information Commissioners Office.

Please note that we may ask you to verify your identity before responding to such requests.

To contact the ICO (Information Commissioner’s Office), phone: 0303 123 1115, email: scotland@ico.org.uk, Wycliffe House, Water Lane, Wilmslow, Cheshire. SK9 5AF.

**Children's Privacy**

WPCS does not address anyone under the age of 13 ("Children"). We do not knowingly collect personally identifiable information from anyone under the age of 13.

If you are a parent or guardian and you are aware that your Child has provided us with Personal Data, please contact us. If we become aware that we have collected Personal Data from children without verification of parental consent, we take steps to remove that information from our servers.

**WPCS Website**

WPCS Website: [www.wpcscotland.co.uk](http://www.wpcscotland.co.uk)

Website Privacy Policy: [WPCS Web Privacy](http://www.wpcscotland.co.uk/index.php/2-uncategorised/238-privacy-policy)

Website Cookies Policy: [WPCS Web Cookies](http://www.wpcscotland.co.uk/index.php/2-uncategorised/239-use-of-cookies)

**Contact Us**

To exercise all relevant rights, and to contact us please use the details below:

Work Place Chaplaincy Scotland

Clydeway House

813 South Street

Glasgow

G14 0BX

Email: info@wpcscotland.co.uk

Phone: 0131 441 2271