Durham Christian Partnership

Data Protection Policy

Policy Number:	**GOV-06**
Scope of this Document (RACI)	**Responsible**: IG Lead **Accountable**: Chief Exec **Consulted**: Office Manager **Informed**: All Staff
Approved By:	Chief Exec
Next Review Date (by):	10/26
Version Number:	1.0
Lead Executive Director:	Chief Exec
Lead Author(s):	IG Lead

Review History	Related Documents to be read in conjunction with
New document in this format. Date as approval date.	Information Security and IT Governance Policies/SOPs
	Privacy and Compliance Policies/SOPs
	Human Resources and Conduct Policies/SOPs
	Operational and Physical Security Policies/SOPs
	Governance and Risk Management Policies/SOPs

This document can be made available via HR request in a range of alternative formats including various languages, large print, high contrast, braille, audio description etc

Approved by Chief Executive on: 13/01/26

Introduction

The organisation (Durham Christian Partnership) uses personal data in the course of providing services, employing staff, communicating with supporters and partners and coordinating volunteer activities. Durham Christian Partnership respects people's rights to privacy and to protection of their personal data. We are registered with the Information Commissioners Office and our registration number is Z713169X. Our registration certificate can be found on the public register at:
https://ico.org.uk/ESDWebPages/Entry/Z713169X

Durham Christian Partnership is committed to compliance with any and all relevant data protection legislation including the UK GDPR/DPA 2018, PECR 2003 and DUAA 2025.

This policy sets out Durham Christian Partnership's overall approach to meeting the legal requirements. Some information is presented in annexes which form part of the policy. Definitions of key terms are provided in annex A.

Scope

This policy applies to all processing of personal data by Durham Christian Partnership which completely or partly involves:

- manual filing systems
- automated means such as computers

Responsibilities of Staff and Volunteers

Staff and volunteers must comply with this policy as well as any supporting procedures and guidance relating to their role. Participation in relevant training is mandatory. Failure to comply will result in disciplinary action.

Unlawful Acts and Criminal Offences

Staff and volunteers should be aware that certain actions constitute criminal offences under data protection law and may lead to police investigation or prosecution. These include, but are not limited to:

- Obtaining, retaining, or disclosing personal data without the consent or lawful authority of the Data Controller.
- Selling personal data or offering or advertising it for sale without authorisation.
- Re-identifying de-identified or anonymised data without the consent of the Data Controller.
- Processing personal data without the consent or other lawful basis established by the Data Controller.
- Altering, concealing, blocking, erasing, or destroying information with the intention of preventing its disclosure, where the individual making a request would have been entitled to receive that information under their rights of access or data portability.
- Requiring individuals to exercise their subject access rights (for example, to obtain copies of their health records, criminal records, or Disclosure and Barring Service (DBS) information) as a condition

of recruitment, employment, service provision, or access to goods or services.

Data Protection Principles

Durham Christian Partnership will process personal data in compliance with Data Protection Principles and will maintain records to demonstrate compliance.

Staff and volunteers are expected to apply the Data Protection Principles below in the context of their role.

1. Lawfulness, fairness and transparency

Durham Christian Partnership will process personal data in a lawful, fair and transparent manner. Durham Christian Partnership will ensure that data subjects receive information about the identity of data controllers and the purposes of processing. Durham Christian Partnership will use clear and plain language to communicate with data subjects and ensure that information about processing of personal data is easily accessible and easy to understand.

2. Purpose limitation

Durham Christian Partnership will collect personal data only for specified, explicit and legitimate purposes and will not further process the data for incompatible purposes. Durham Christian Partnership may carry out further processing for the purposes of the public interest, scientific or historical research or statistical purposes.

3. Data minimisation

Durham Christian Partnership will ensure that personal data is adequate, relevant and limited to what is necessary to achieve the purposes for which they are processed. Durham Christian Partnership will not process personal data unless it is needed to fulfil these purposes.

4. Accuracy

Durham Christian Partnership will ensure that personal data is accurate and updated where necessary. Durham Christian Partnership will rectify or delete inaccurate personal data without delay.

5. Storage limitation

Durham Christian Partnership will keep personal data in a form that makes it possible to identify data subjects for no longer than is necessary for the purposes of the processing. If data is retained for longer periods for purposes in the public interest, scientific or historical research purposes or statistical purposes, Durham Christian Partnership will safeguard the rights and freedoms of data subjects.

6. Integrity and Confidentiality

Durham Christian Partnership will ensure that the manner of processing ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Lawfulness of processing

Durham Christian Partnership staff and volunteers may only process personal data using approved Durham Christian Partnership processes; failure to comply may result in disciplinary and/or police action.

In designing its processes, Durham Christian Partnership will establish the lawful basis for any processing of personal data. Conditions for lawful processing are summarised in annex B.

In the case of sensitive personal data (see annex A), Durham Christian Partnership will identify additional justification for lawful processing. Legal criteria for processing sensitive personal data are shown in annex C.

Durham Christian Partnership will consider the detailed requirements of the legislation and regulations where clarification is required.

Rights of Data Subjects

Legal rights of data subjects are explained in annex D.

Durham Christian Partnership has a legal responsibility to make it easy for data subjects to exercise their rights. All staff and volunteers are expected to contribute to this.

The law requires data controllers to communicate with data subjects about processing:

- in a concise, transparent, intelligible and easily accessible way using clear and plain language.
- by any appropriate means including:
  - orally, when this is requested by the data subject, subject to identity being proven by other means
  - electronically, where personal data are processed by electronic means
- free of charge, except where requests are clearly unfounded or excessive when a charge may be made to cover administrative costs or the request may be refused.

Durham Christian Partnership will prepare Privacy Notices which explain how Durham Christian Partnership complies with the law and enables data subjects to access their rights.

When collecting personal data or advising about rights, staff and volunteers must tell data subjects about the availability of the relevant Privacy Notice.

Data controllers must respond to requests from data subjects without undue delay and at the latest within one month and give lawful reasons if it does not intend to comply with requests.

If a member of staff or volunteer receives a query that they are unable to resolve, they should seek support from their supervisor, team leader or manager

Data Controller and Data Processor roles

Durham Christian Partnership may act as a controller, joint controller or processor. The role affects how processes are developed and operated.

Legal responsibilities of controllers and processors are listed in annex E.

The respective responsibilities of joint controllers for compliance should be made clear in a formal agreement. Joint controllers bear joint liability in the event of a data breach.

A processor should process personal data in accordance with purposes and means determined by the controller. If a processor strays beyond the role by determining purposes and means, then the law considers it to be a controller.

Data protection by design and default

A controller has a duty to

- consider risks including possible impacts on the rights and freedoms of individuals;
- take appropriate technical and organisational measures to protect data subjects and their rights;
- implement these measures to ensure data protection by design and default.

Data processing risks, risk assessment and general approaches to mitigate risk are identified at annex F.

Staff or volunteers who develop processes for personal data should apply the principles for privacy by design presented at annex G.

Data Protection Impact Assessment

Durham Christian Partnership may conduct a data protection impact assessment (DPIA) to identify the origin, nature, specific details and severity of risks.

The law requires a DPIA for: automated evaluation of persons; large scale processing of sensitive personal data and systematic monitoring of a publicly accessible area on a large scale.

A DPIA must at minimum include:

- systematic description of the processing operations, purposes and, where applicable, the legitimate interest pursued by the controller
- assessment of the necessity and proportionality of the processing operations in relation to the purposes
- evaluation of the risks to the rights and freedoms of data subjects
- possible measures to address risks and demonstrate compliance

Where a DPIA indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk, a controller must consult the ICO prior to processing.

Transferring data outside the European Union

Durham Christian Partnership may transfer personal data to countries outside the European Economic Area if:

- the European Commission has assessed that the location provides an adequate level of data protection;
- Durham Christian Partnership provides appropriate safeguards and there are enforceable data subject rights and effective legal remedies in the country; or
- the circumstances of the transfer are specifically permitted by law.

Record keeping

Durham Christian Partnership will maintain written records, which it will make available to the ICO on request, of:

- the names and contact details of relevant controllers and processors
- where Durham Christian Partnership is the data controller:
  - the purposes of the processing
  - categories of data subjects, personal data and recipients
  - envisaged time limits for erasure of the different categories of data
- Where Durham Christian Partnership is the data processor:
  - Categories of processing carried out on behalf of each controller
- A description of technical and organisational security measures, where possible
- Any transfer of data outside the EU and related safeguards

Complaints

Durham Christian Partnership will provide a complaints process aligned with its complaints policy which provides for: investigation as appropriate; updating on progress; information on the outcome; information on the right to escalate a complaint to the ICO.

Providing information when collecting personal data

A controller must provide certain information to data subjects when collecting personal data. Durham Christian Partnership will meet this obligation by including the information in a Privacy Notice. Durham Christian Partnership will also include information about its complaints process. The minimum contents of a Privacy Notice are listed at annex H.

Dealing with a data breach

There is a risk of personal data breach due to an intentional attack on Durham Christian Partnership's systems or the unintentional errors of staff and volunteers.

In view of the possible impacts on data subjects, the law sets tight deadlines for notification of breaches. The co-operation of staff and volunteers is vital to achieving these deadlines. A member of staff or volunteer who becomes aware of a data breach must notify the Chief Executive of Durham Christian Partnership or nominated representative ***immediately***.

The Chief Executive will consider the need for notifications to be made in accordance with annex I.

Registration with the ICO

Durham Christian Partnership will monitor whether registration with ICO is required and, if so, shall register and pay the appropriate fee.

Data Protection Officer

A Data Protection Officer must be appointed if:

- processing is carried out by a public authority or body
- core activities involve regular and systematic monitoring of data subjects on a large scale
- core activities consist of large-scale processing of sensitive personal data or data relating to criminal convictions or offenses

Durham Christian Partnership does not consider it necessary to appoint a dedicated Data Processing Officer.

Working with Data Processors

If Durham Christian Partnership considers hiring a new Processor, it will check whether the Processor has obtained certification to any security-related standard and ask the potential Processor for evidence of their data security procedures.

A contract will be put in place with a new Processor requiring that the Processor will:

- process the personal data only on documented instructions from Durham Christian Partnership
- ensure that persons authorised to process the personal data are committed to confidentiality
- keep the data secure
- not hire another Processor to do the work without permission of Durham Christian Partnership
- help Durham Christian Partnership to fulfil requests from data subjects enforcing their rights
- help Durham Christian Partnership to fulfil legal and regulatory duties including breach notification requirements
- delete or return the personal data at the end of the contract, as required by Durham Christian Partnership
- provide information to demonstrate compliance including allowing their processes to be inspected and audited

Contact

Any queries about Durham Christian Partnership's approach to data protection should be addressed to:

The Chief Executive Officer

Organisation Durham Christian Partnership

Address
Unit 7-9
1st Avenue
Drum Ind Est
DH2 1AG

Email; office@durhamcp.org.uk

Annex A

Definitions

"Personal data" means any information about an identified or identifiable living person, called "a data subject". The person might be identifiable directly (by their name or other identifier) or indirectly (through location data and/or other factors specific to the person).

"Sensitive personal data" reveals:

1. racial or ethnic origin
2. political opinions
3. religious or philosophical beliefs
4. trade union membership
5. genetic data
6. biometric data used to identify people (e.g. facial images and voice recordings)
7. health data
8. data concerning individual's sex life
9. sexual orientation

“Filing system” means a structured set of personal data which is accessible according to specific criteria, which may be automated or manual and which may be centralised or dispersed on a functional or geographical basis.

"Processing" means any operation on personal data, whether or not by automated means, such as:
(a) collection, recording, organisation, structuring or storage
(b) adaptation or alteration
(c) retrieval, consultation or use
(d) disclosure by transmission, dissemination or otherwise making available
(e) alignment or combination, or
(f) restriction, erasure or destruction

A "data controller" or "controller" is the natural or legal person who determines the purposes and means for processing personal data.

A "data processor" or "processor" engages in the processing of personal data on behalf of a data controller.

"ICO" means the Information Commissioner's Office. Data controllers and data processors are accountable to the ICO for their data processing.

Annex B

Conditions for lawful processing of personal data

Processing is lawful where at least one of the following applies:

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

- Consent means an indication of the data subjects' wishes that is given freely and is specific, informed and unambiguous. Consent can be granted by a statement or by a clear affirmative action.

- Records to demonstrate consent must be maintained. Where a written declaration is used, the request for consent to processing must be distinguished from any other matters. The request must be presented in an intelligible and easily accessible form and use language which is clear and easy to understand.

- Data subjects may withdraw their consent to future processing at any time. Before a person gives consent, they must be informed about the possibility of withdrawing it. Withdrawing consent must be made as easy as giving it.

- For a child under 13, the request for consent must be made to the parent or legal guardian.

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

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

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

(e) 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 controller;

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

- The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller.

Annex C

Conditions for lawful processing of sensitive personal data

Sensitive personal data may not be processed unless (at least) one of the conditions listed in annex B is met and, in addition, (at least) one of the following conditions applies -

(a) the data subject has given explicit consent, except where law prevents this;

(b) processing is necessary to meet obligations and specific rights relating to employment, social security and social protection law;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on a legal basis and subject to suitable safeguards;

(h) processing is necessary for medical purposes, assessment of working capacity, health and social care, or under contract with a health professional where the processing is under the responsibility of a person who is subject to an obligation of secrecy under law or rules established by national competent bodies;

(i) processing is necessary for reasons of public interest in the area of public health;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to legal safeguards;

Processing of personal data about criminal convictions and offences or related security measures may only be carried out with specific legal authorisation and safeguards.

Annex D

Rights of Data Subjects

Right of access

Data subjects have a right to confirmation of whether or not a data controller is processing their personal data and, if so receive:

- a copy of the personal data
- the purposes of the processing
- the categories of the personal data
- the recipients or categories of recipient of the personal data
- the storage period, or criteria to determine the storage period
- existence of the rights to rectification, erasure, restriction of processing or objection
- the right to lodge a complaint with the Information Commissioner's Office
- any information about the source of the personal data, if not the data subject
- the existence of any automated decision making and information about this
- relevant safeguards, if data is transferred to a third country

If a request to access personal data is made by electronic means, the controller should respond in electronic form unless the data subject specifically requests otherwise. The controller must provide a first paper copy free; for any additional copy, the controller may charge a fee based on administrative costs.

The right to obtain a copy may not adversely affect the rights and freedoms of others.

Right to rectification

Data subjects have the right to:

- rectification of inaccurate information about them without undue delay
- have incomplete personal data completed, including by supplementary statement

Where the data subject has exercised their right to rectification, the controller shall communicate this to each recipient of the personal data (unless impossible or disproportionate effort). The controller shall inform the data subject about those recipients if the data subject requests it.

Right to object

Data subjects have a right to object to further processing of their personal data where the legal basis for the processing is that it is necessary for: tasks performed in the public interest; or the legitimate interests of a data controller or a third party.

In such situations, the controller must indicate the existence of the right to object:

- at the time of the first communication with data subjects
- in a clear manner and separately from other information.

If a data subject exercises the right to object, the controller must cease the processing if there are no compelling legitimate grounds for continuing it and processing is not needed in relation to legal claims.

Right to restriction of processing

Data subjects have a right to obtain restriction of processing from the controller where:

- accuracy of personal data is contested - for a period enabling verification;
- processing is unlawful, and data subjects request restriction rather than deletion;
- controllers no longer need the data for the purposes of the processing but the data are required by data subjects for legal claims;
- data subjects object to the processing pending verification of whether the legitimate grounds of data controllers override those of data subjects.

If one of these conditions applies, the controller may only continue processing:

- with the consent of the data subjects;
- in relation to legal claims;
- for the protection of the rights of others;
- for reasons of important public interest.

Where the data subject has exercised their right to restriction of processing the controller shall communicate this to each recipient of the personal data (unless impossible or disproportionate effort). The controller shall inform the data subject about those recipients if the data subject requests it.

Where a restriction of processing has been obtained, the controller will inform data subjects before the restriction is lifted.

Right to erasure

Data subjects have a right to erasure of their personal data by the controller without undue delay if:

- the data are no longer needed for the relevant purposes;
- data subjects withdraw consent and there is no other legal basis for processing
- data subjects object to processing and there are no overriding legitimate grounds for the processing
- personal data have been unlawfully processed
- personal data must be deleted to comply with a legal obligation
- personal data have been collected in relation to the offer of any service which is normally requested by an individual at a distance via electronic means and paid for.

Where a controller has disclosed data which it obliged to erase, it must take reasonable steps to inform other relevant controllers that the data subject has requested erasure of any links to or copies of the data.

The right to erasure does not apply where processing is necessary:

- to exercise of the right to freedom of expression and information
- to comply with a legal obligation
- for a task carried out in the public interest
- for scientific, historical research or statistical purposes
- in relation to legal claims

Where the data subject has exercised their right to erasure, the controller shall communicate this to each recipient of the personal data (unless impossible or disproportionate effort). The controller shall inform the data subject about those recipients if the data subject requests it

Right to data portability

This right to obtain data portability from a data controller exists where:

- the data subject has provided the personal data
- processing is based on consent or on a contract
- processing is carried out by automated means
- the data is not used for tasks carried out in the public interest or in the exercise of official authority

The right may not be used to adversely affect the rights and freedoms of others.

Where the data subject exercises their right to data portability, the controller must provide their personal data in a structured, commonly used and machine-readable format and, where technically possible, transmit these data to another controller.

Right to lodge a complaint with a supervisory authority

Data subjects have the right to lodge a complaint about the processing of their personal data with the Information Commissioner's Office.

Right not to be subjected to a decision based only on automated processing

Data subjects have the right not to be subjected to a decision based only on automated processing which has legal or other significant consequences for the data subject, except where an automated decision:

a. is needed in relation to a contract between the data subject and the controller;
b. is authorised by a law which provides suitable safeguards; or
c. is based on the explicit consent of the data subject

In cases a and c, the controller shall implement suitable safeguards of rights, freedoms and legitimate interests: at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

Automated decisions must not be based on sensitive personal data unless done:

- with the consent of the individuals involved
- for reasons of substantial public interest

Where decisions are based on automated processing, measures must be introduced to safeguard data subjects' rights, freedoms and legitimate interests.

Annex E

Responsibilities of Data Controllers and Data Processors

Data Controllers must:

- implement measures, including appropriate policies, to ensure and demonstrate processing in accordance with the law
- demonstrate its compliance with the data processing principles
- consider the nature, scope, context and purposes of processing and risks including possible impacts on the rights and freedoms of individuals
- take appropriate technical and organisational measures to protect data subjects and their rights, and implement these measures to ensure data protection by design and default
- maintain records of data processing activities to demonstrate legal compliance
- ensure a level of security appropriate to the risk in processing data
- co-operate with the ICO as appropriate and notify the ICO in the event of a breach
- conduct data protection impact assessments where there is high risk
- consider whether there is a requirement to appoint a Data Protection Officer
- meet legal obligations regards transfer of any data outside the EU
- assist data subjects with exercising their rights to privacy and data protection, including providing information when collecting personal data

Data Processors must:

- comply with the contract (or similar act) which clarifies the processing details and, as required by the contract,
  - act on written instructions from the data controller
  - ensure confidentiality, assist the controller to comply with the law and respond to requests from data subjects
  - provide information to demonstrate compliance of the controller
  - assist the controller with ensuring security of processing
  - treat personal data after processing as directed by the controller
- comply with the data processing principles
- protect the rights and freedoms of data subjects
- demonstrate compliance with legislation
- maintain records of processing and make them available to the ICO on request
- consider need to appoint a Data Protection Officer
- cooperate with ICO as appropriate
- take appropriate technical and organisational measures to ensure security and protect the rights of data subjects
- meet specific obligations regarding transfer of data outside the EU

Annex F

Data processing risks, risk assessment and general approaches to mitigate risk

Risks include accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access to personal data transmitted, stored or otherwise processed.

Assessment of the level and impact of risks should include consideration of the volume of personal data, the number of data subjects concerned and the possibility of:

- discrimination
- identity theft or fraud
- financial loss
- damage to reputation
- loss of confidentiality of personal data protected by professional secrecy
- unauthorised reversal of pseudonymisation
- other significant economic or social disadvantage
- damage to data subjects' rights and freedoms or exercise of control over their data
- unauthorised use or disclosure of sensitive personal data or data about vulnerable people and children in particular
- unauthorised use or disclosure of data which may be used for evaluation such as performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements

The approach to mitigating risk should take into account:

- the nature, scope, context and purposes of processing
- the state of the art
- implementation cost
- the likelihood and severity of risks for the rights and freedoms of individuals

Measures to mitigate risk may include:

- Transparency with regard to the functions and processing of personal data
- Minimisation of the collection, processing and storage of personal data
- Anonymisation – where ways of identifying the data subject are irreversibly destroyed and the data subject cannot be re-identified either directly or indirectly
- Pseudonymisation – where additional data is required to re-identify the data subject: this may include replacement of personal details by a code
- Encryption
- Steps to ensure people acting for controller/processor do not process personal data except on instructions from the controller (except where the law requires)
- Authentication and authorisation mechanisms
- Ensuring the ongoing confidentiality, integrity, availability and resilience of systems and services
- Ability to restore the availability and access to personal data in the event of a physical or technical incident
- Arrangements for confidential disposal and destruction of personal data
- Regularly testing the security measures

Annex G

7 Foundational Principles for Privacy by Design

1. A ***proactive and preventative approach*** which aims to address risks of invasion of privacy and prevent these rather than on remedies after the event.

2. ***Privacy as the default*** - The purpose for processing the information will be clearly communicated to the person concerned. The collection of information shall be fair, lawful, limited to that purpose and the strict minimum required for that purpose. The processing, storage period and accessibility of the data shall be limited to that purpose and, when that processing is complete, the data shall be destroyed.

3. Privacy ***embedded*** into design – with consideration of privacy risks and measures to mitigate those risks from the outset as an integral part of the development of processes (see annex F).

4. ***Full*** functionality – design which accommodates all legitimate objectives including technical capabilities, privacy and security.

5. ***End to end security*** to assure the confidentiality, integrity and availability of personal data throughout its lifecycle including methods of secure destruction.

6. **Visibility and transparency** to verify that processing happens according to stated promises and objectives. This includes clear accountability, making information about policies and practices available, a complaint process and steps to check compliance.

7. **Respect for user privacy** – to keep the interests of the individual uppermost during process design. Processes should:
    - be user friendly
    - enable informed decisions about consent
    - maintain accuracy of information
    - enable individuals to
    - access information and be informed about its uses and disclosures
    - challenge the accuracy of the information and have it amended
    - communicate opportunities for complaint and redress

Reference

Privacy by Design, The 7 Foundational Principles, Implementation and Mapping of Fair Information Practices. Ann Cavoukian, Ph.D. Information & Privacy Commissioner, Ontario, Canada. **https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf**

Annex H

Minimum content for a Privacy Notice

On collecting personal data directly from data subjects, a controller must provide information on:

- The controller's identity and contact details
- The contact details of the person responsible for data protection
- The purposes and legal basis for the data processing
- The reason why the data subject needs to provide personal data, whether the data subject is obliged to provide the data and the consequences of not doing do
- The recipients of the personal data
- Whether the controller intends to transfer personal data outside the EU
- The data storage period
- Data subjects' rights: access, rectification, erasure, restriction of processing, objection to processing, data portability, right to withdraw consent, opportunity to lodge a complaint with Durham Christian Partnership, right to lodge a complaint with the ICO
- The existence of any automated decision making, including profiling
- Whether the controller intends to further process the data for a purpose other than that for which the data is initially collected

If personal data is collected indirectly, the controller must provide data subjects with

- the information listed above
- details of the categories of personal data
- the source.

unless

- the data subject already has the information
- doing so would be impossible or incur disproportionate effort
- doing so would make impossible or seriously impair achievement of the processing objectives
- the law provides measures to protect the legitimate interest of data subjects
- the data is subject to a legal obligation of professional secrecy.

Annex I

Notifications by the Chief Executive in the event of a Data Breach

A member of staff or volunteer who becomes aware of a data breach must notify the Chief Executive of Durham Christian Partnership or nominated representative ***immediately***. The Chief Executive will then consider the need for notification of the ICO, a data controller and data subjects.

(a) Notification of the ICO

If Durham Christian Partnership is the data controller, it will notify the ICO about a breach, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. Durham Christian Partnership will make the notification without delay and, where feasible, within 72 hours of becoming aware of it. If notification is not within 72 hours, Durham Christian Partnership will indicate the reasons for the delay. The notification shall include:

- the nature of the breach including, where possible, the categories and approximate number of data subjects and the categories and approximate number of records
- the name and contact details where more information can be obtained
- the likely consequences of the personal data breach
- the measures taken or proposed to be taken to address the breach including any measures to mitigate possible adverse effects

To minimise delay, Durham Christian Partnership may provide this data in phases.

Measures taken to address a breach may include:

- prompt action to mitigate the damage suffered by data subjects
- notification, communication and co-operation with the ICO to remedy the failure and mitigate possible adverse effects
- communication with the data subject
- review of practice to achieve security, data protection by design and default and legal compliance

Durham Christian Partnership will record any such breach including facts relating to the breach, its effects and remedial action taken and make this record available to the ICO to verify compliance.

(b) Notification of a data controller

As a processor, Durham Christian Partnership will notify the controller of a breach without undue delay. If Durham Christian Partnership engages a processor, it will require the processor to notify it of breaches without undue delay.

(c) Notification of data subjects

If Durham Christian Partnership is the data controller, it will communicate to data subjects in clear, plain and understandable language the same information given to the supervisory authority unless:

- appropriate measures such as encryption have been applied
- subsequent measures prevent high risk to rights and freedoms of data subjects
- disproportionate effort would be required and a public communication or similar measure would be sufficient to inform data subjects