Data Protection Policy

Contact Details: Unit 24, SHBP, Majors Road, Watchfield, SN6 8TZ; 01793 783123

The prudent keep their knowledge to themselves, but a fool's heart blurts out folly. (NIV – Prov 12:23)

1. ICO Reference

Reference Number – ZB179985. Date of Renewal 24 August 2022.

All organisations which process personal data must be registered with the Information Commissioner’s Office (ICO). Currently, the Cornelius Trust is registered with the ICO for the following purposes:

• Accounts and Records

• Advertising, Marketing and Public Relations

• Staff Administration

• Fundraising

• Realising the Objectives of a Charitable Organisation or Voluntary Body

1. Introduction, Scope and Context
   1. Introduction

This document sets out the policy, practice and responsibilities adopted by the Cornelius Trust to meet its legal obligations under the UK’s Data Protection Act 2018 (DPA 2018). This came into effect on 25 May 2018 to reflect new regulations under EU Regulation 2016/679 General Data Protection Regulation (EU GDPR).

This policy should be read in conjunction with other Cornelius Trust UK GDPR compliance documents, such as the website privacy statements which set out how data relating to individuals is used by the Cornelius Trust in the course of its charitable business.

* 1. Scope

This policy describes how personal data must be collected, handled, processed, transferred and stored to meet the standards set by the Board of Trustees and to comply with the law.

It applies to all Cornelius Trust trustees, associated organisations, suppliers and other people the Trust has a relationship with or may need to contact.

This policy applies to all data held by the Cornelius Trust relating to identifiable individuals (i.e. ‘natural persons’). The test to apply to determine whether or not someone is ‘identifiable’ is as follows:

• Is a natural person identified or are they identifiable, directly from the information in question; or

• Is a natural person indirectly identified from that information in combination with other information (e.g. computer IP addresses).

This can include:

• Names of individuals

• Rank and service number of individuals

• Postal addresses

• Email addresses

• Telephone numbers

• Gender

• Marital status

• Names and ages of children (where appropriate)

• Other personal relevant information

* 1. Context

The UK GDPR describes how organisations including the Cornelius Trust must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or other materials. To comply with the law, personal information must be collected, used fairly, stored safely and not disclosed unlawfully. We recognise too that the correct and lawful treatment of personal data maintains confidence in the Charity.

1. Definition of Data Protection Terms
   1. Data

This is information which is stored electronically, including on a computer or 'in the cloud', or in certain paper-based filing systems.

* 1. Data subjects

For the purpose of this policy these include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

Information about a deceased person does not constitute personal data and therefore is not subject to the UK GDPR.

* 1. Personal data

This means data relating to a living (‘natural’) individual (‘data subject’) who can be identified from that data (or from that data and other information in our possession) whether directly or indirectly. Personal data can be factual (e.g., a name, address, date of birth, identify number or online identifier); it can refer to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person; or it can be an opinion about that person, their actions and behaviour.

* 1. Data controllers

These are the people who or entities which determine the purposes and the manner in which any personal data is processed. They are responsible for establishing practices and policies in line with the Act. We are the data controller of all personal data used in the running of the Cornelius Trust.

* 1. Data users

These are those of our trustees and associated organisations whose work and service involve processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data/ IT security procedures at all times.

* 1. Data processors

These include any person or entity that is not a data user who/ that processes personal data on our behalf and on our instructions. Staff of data controllers are excluded from this definition, but it could include third parties which handle personal data on the Cornelius Trust’s behalf.

* 1. Processing

This is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including collecting, structuring, organising, amending, retrieving, using, disclosing, disseminating, erasing or destroying it. Processing also includes transferring personal data to third parties.

* 1. Sensitive personal data

This includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned. In order to process these types of data consent from the data subject must be obtained by the organisation handling the data. Explicit consent must be given when it is sensitive personal data.

The term ‘personal data’ used throughout this policy should be taken to include both kinds of ‘personal’ and ‘sensitive personal’ data.

1. Responsibilities
   1. Who is responsible?

The Cornelius Trust will do its utmost to ensure that all its trustees, members and third-party suppliers are conversant with data protection legislation and practice.

Everyone who works for or with the Cornelius Trust, whether on a paid or voluntary basis, has some responsibility for ensuring data is collected, stored and handled appropriately. However, certain people have key areas of responsibility.

* 1. Board of Trustees

The Board of Trustees is ultimately responsible for ensuring the Cornelius Trust meets its legal obligations.

* 1. Data Protection Officer

The Cornelius Trust Secretary is the Data Protection Officer (DPO) with overall responsible for the implementation of this policy, in particular:

• Keeping the Board updated about data protection responsibilities, risks and reviews, contributing to periodic reports, meetings, etc as needed

• Reviewing all data protection procedures and related policies in line with the agreed schedule and keeping them up-to-date, including to reflect any new legal developments

• Arranging data protection training and advice for people covered by this policy

• Handling data protection questions from staff and anyone else covered by this policy

• Ensuring that the Cornelius Trust’s database and all other processes (whether in electronic or other form) are maintained in a data protection compliant manner

• Ensuring that adequate insurance is in place should any data breaches occur, and that all requirements for insurance cover to be valid (e.g., the existence of certain policies or procedures required for any cyber and data breach insurance) are met

• Ensuring that the Cornelius Trust’s registration with the Information Commissioner’s Office is kept up-to-date and renewed annually

• Ensuring that all data protection registers, records, forms, etc required by law or representing good practice are maintained and kept up-to-date

• Dealing with requests from individuals in relation to the data Cornelius Trust holds about them (e.g., Subject Access Requests for erasure or correction – see further sections 11 and 12 below)

• Checking and approving any contracts or agreements with third parties that may handle the Trust's data

• Approving any data protection statements attached to communications such as emails or letters

• Addressing any data protection queries from outside agencies (including journalists, media outlets or the ICO)

• Ensuring all marketing and promotional initiatives abide by data protection principles

* 1. IT Provider

Tapatalk is responsible for:

• Ensuring all systems, services and equipment used for storing data meet acceptable security standards

• Performing regular checks and scans to ensure security hardware and software is functioning properly

• Approving and recommending software to prevent malicious threat and data theft

1. Use of Personal Information
   1. Personal information held

The Cornelius Trust holds personal information about living individuals, especially trustees, supporters and other individuals who have provided such information for specific purposes relating to the work of the Trust.

During the course of our activities we collect, store and process personal data about past, current and prospective members and other third parties with whom we communicate.

* 1. Use of personal information

The principal purposes for which this personal information is used include:

• The day-to-day administration of the Cornelius Trust, such as maintaining financial records for audit, tax and Gift Aid purposes

• Maintaining confidential records of Cornelius Trust trustees

• For the purposes of legal proceedings

• For compliance with legislation

All personal information which is held by the Cornelius Trust will be treated as private and confidential and only disclosed to those persons involved in the administration and day-to-day work of the Cornelius Trust, unless otherwise agreed with the data subject.

* 1. Data protection risks

This policy is important not only because it helps us to meet our legal compliance obligations, but also due to the real risks associated with the handling and use of data. These can take many forms, for instance:

• Breaches of confidentiality which can undermine trust and hinder the fulfilment of our charitable mission

• Reputational damage which can impact negatively upon our support base

• Inappropriate use of personal data which does not offer genuine choice to individuals concerning how their data is used, thereby undermining trust

• Insufficient security measures which lead to a data breach which could cost the Trust significant sums of money in terms of ICO fines, personal data monitoring, etc

1. Data Protection Principles

The Cornelius Trust fully endorses and adheres to the principles of good practice of the UK GDPR detailed below. These principles specify the legal conditions that must be satisfied in relation to obtaining, handling, processing, transportation and storage of personal data. All persons and other entities covered by the scope of this policy, who obtain, handle, process, transport and store personal data for the Cornelius Trust, must adhere to these principles.

Seven principles lie at the heart of the general data protection regime. These are that all personal data must be:

• Processed fairly, lawfully and in a transparent manner

• Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

• Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This does not mean that the processing of data has to be essential; rather that it must be a targeted and proportionate way of achieving the stated purpose of the processing of any data

• Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay

• Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. This will depend on various factors, such as legal limitation or specified periods we are required or advised to retain records for

• Processed in a manner that ensures appropriate security of the personal data to protect its integrity and confidentiality, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

• Accountability, namely that any data controllers or processors take responsibility for complying with these principles, and have appropriate processes and records in place to demonstrate that compliance

1. Lawful, Fair and Transparent Data Processing

Data protection legislation is not intended to prevent the processing of personal data, but rather to ensure that it is done lawfully, fairly and transparently, without adversely affecting the rights of the data subject. Its provisions are more extensive than those of the Data Protection Act 1998, with the UK GDPR placing more emphasis on accountability for and transparency about the lawful basis relied upon for data processing.

For personal data to be processed lawfully, they must be processed on the basis of one or more of the legal grounds set out in the UK GDPR. These specified legal bases are as follows:

• Consent: the Cornelius Trust has been given clear consent for us to process personal data for a specific purpose.

• Contract: the processing is necessary for a contract we have with the data subject or because they have asked us to take specific steps before entering into a contract.

• Legal obligation: the processing is necessary for us to comply with the law (not including contractual obligations).

• Vital interests: the processing is necessary to protect someone's life.

• Public task: the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.

• Legitimate interests: the processing is necessary (i.e. conducted in a targeted and proportionate way) for our legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the data subject’s personal data which overrides those legitimate interests (i.e. a balancing test has been undertaken between our legitimate interests and your interests, rights and freedoms to assess whether your interests override our legitimate interests). When this legal basis is relied upon, we are under an obligation to keep it under review.

1. Processing of Sensitive Data

As a general approach, we do not collect special categories of personal data (formerly known as ‘sensitive data’). Examples of special category data include information about an individual's: race; ethnic origin; politics; religion; trade union membership; genetics; biometrics; health; sexual orientation; or unspent criminal convictions.

We may use information relating to criminal convictions where it is necessary in relation to legal claims.

Any such processing will be in accordance with this Data Protection policy.

1. Keeping Data Subjects Informed

The Cornelius Trust shall provide the following information to all of its data subjects:

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

• Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose when the first communication is made with them, before any transfer is made, or as soon as reasonably possible (and not more than one month after the personal data is obtained).

Furthermore, all data subjects will be provided with the following details: the legal basis (legitimate interest relied upon); the category of personal data collected and processed; any third parties to whom data is transferred; data retention; and the data subject’s rights under UK GDPR (e.g., to withdraw their consent, or to complain).

The Cornelius Trust aims to ensure that individuals know what data is being held, and they understand:

• How the data is being used

• How to exercise their rights

• How to restrict the amount and type of data that is shared with other members

1. Processing in Line with Data Subject’s Rights

We will process all personal data in line with data subjects' rights, in particular their:

• Right to be informed about the collection and use of their personal data

• Right of access to any data held about them by a data controller (see also clause 11)

• Right to rectification (see also clause 12)

• Right to erasure (see also clause 12)

• Right to restrict processing (see also clause 12)

• Right to data portability (see also clause 12)

• Right to object (see also clause 12)

1. Dealing with Subject Access Requests
   1. What is a Subject Access Request (SAR)?

All Cornelius Trust data subjects may make a Subject Access Request (SAR) at any time to find out more about the personal data which the Charity holds about them, what it is doing with that personal data, and why.

Data subjects may make a SAR either orally or in writing. This request must relate to their personal data only; the personal information relating to other people cannot normally be requested. Any Cornelius Trust trustees receiving a written request should forward it to the DPO immediately.

* 1. What Data may be Requested?

Data subjects have the right to obtain the following information from us:

• Confirmation that we are processing their personal data

• A copy of their personal data

• Other supplementary information

* 1. Conditions to be met for a SAR

In making a SAR orally, the following conditions need to be met:

• We will check the caller's identity to make sure that information is only given to a person who is entitled to it. Such identity confirmation should involve verifying at least three items of personal data, such as date of birth, home address, personal phone number

• We will require that the caller puts their request in writing if we are not sure about the caller’s identity and where their identity cannot be checked

• A standard SAR form is at Appendix 1 to this policy. It is not, however, essential for this form to be used. SARs may be made by any means, e.g. in the form of a letter, email or orally.

* 1. Legalities

Under UK GDPR, we have one month in which to respond to such a request, acting without undue delay. If the request is complex or if multiple requests from the same person have been received, we may extend the time to respond by a further two months.

Normally, no fee will be charged to comply with the SAR, unless it is considered to be manifestly unfounded or excessive, or further copies of data are requested following a request. In such circumstances, a 'reasonable fee' may be charged for the administrative costs associated with complying with the request.

In certain circumstances, we can refuse to respond to a request (e.g., if it would disclose information about another individual who can be identified from the information unless, for instance, that person has consented to such disclosure; or if the request is manifestly unfounded or excessive); or we can extend the time limit to respond to a request (e.g., due to its complexity).

1. Dealing with other Requests

Under the UK GDPR, there are a number of other requests which data subjects may make which are outlined briefly here.

* 1. Request for rectification

This is the right to have inaccurate personal data rectified or completed if it is incomplete. Personal data is inaccurate if it is incorrect or misleading as to any matter of fact.

* 1. Request for erasure

This is the right for data subjects to have personal data erased, otherwise known as “the right to be forgotten.” This applies in certain circumstances, such as if:

• The personal data is no longer necessary for the purpose for which the Cornelius Trust originally collected or processed it

• If consent, forming the legal basis for holding data, is withdrawn by the data subject

• The data subject objects to the holding and processing of their personal data (and there is no overriding legitimate interest to allow the Cornelius Trust to continue doing so)

• The personal data has been processed unlawfully, or

• The personal data needs to be erased (or in some instances not erased) in order for the Cornelius Trust to comply with a particular legal obligation

In certain circumstances, the right to erasure will not apply if processing is necessary:

• To exercise the right of freedom of expression and information

• To comply with a legal obligation

• For the establishment, exercise or defence of legal claims

* 1. Request to restrict processing

This is the right of a data subject to request the restriction or suppression of their personal data in certain circumstances as an alternative to requesting the erasure of their data.

This right may be exercised in certain circumstances, including:

• If the data subject contests the accuracy of their personal data and the Cornelius Trust is verifying the accuracy of the data

• The data has been unlawfully processed (i.e. in breach of the lawfulness requirement of the first principle of the UK GDPR)

• The Cornelius Trust no longer needs the personal data, but the data subject needs to keep it in order to establish, exercise or defend a legal claim

• The restriction of data may take a number of different forms, for instance:

• Temporarily moving the data to another processing system

• Making the data unavailable to users, or

• Temporarily removing published data from a website

* 1. Request to data portability

The right to portability allows data subjects to obtain and reuse their personal data for their own purposes across different services. For instance, it allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.

The data should be supplied in a manner that is structured (i.e. allows for easier transfer and increased usability), commonly used (i.e. widely used and well-established) and in machine-readable (i.e. can be automatically read and processed by a computer) format. This right only applies to information an individual has provided to a data controller.

The right to data portability only applies when the legal basis for holding personal data is consent or the performance of a contract, or the Cornelius Trust is carrying out data processing by automated means.

* 1. Dealing with an objection

The UK GDPR gives individuals the right to object to the processing of their personal data in certain circumstances. They have an absolute right to object if the processing of their data is for direct marketing purposes.

The timelines, format, restrictions, and (non) payment of fees are very similar to those for Subject Access Requests.

1. Data Security

The Cornelius Trust takes appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

We will put in place appropriate technological and organisational measures (such as organisational policies, physical or technical measures) to maintain the security of all personal data from the point of collection to the point of destruction as is required by the UK GDPR.

We will maintain data security by protecting the confidentiality, integrity and availability of the personal data. This includes through the implementation of office routines and protocols, such as file sharing rather than emailing personal information, good email and electronic filing housekeeping, appropriate use of privacy markings such as “confidential”; as well as through various security measures such as passwords, encryption, regular back-ups, use of lockable storages, shredding, etc.

1. Personal Data Breaches
   1. Duty to Report Personal Data Breaches

The UK GDPR requires the Cornelius Trust to report certain types of personal data breach to the relevant supervisory authority within 72 hours of becoming aware of the breach, where feasible. Where the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, we must inform data subjects of this without undue delay.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data.

It means that a breach of security has occurred leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

* 1. Examples of Data Breaches

Specific examples of common personal data breaches are:

• Access by an unauthorised third party

• Deliberate or accidental action (or inaction) by a controller or processor

• Sending personal data to an incorrect recipient

• Computing devices containing personal data being lost or stolen

• Alteration of personal data without permission, and

• Loss of availability of personal data

It is essential that the DPO is notified immediately anyone (e.g., data subject or Cornelius Trust trustee) becomes aware of any suspected breach of personal data. If the breach is likely to pose a risk to the data subject (e.g., emotional distress, physical and/or material damage such as financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage) then the Information Commissioner’s Office must be notified.

1. Transferring Personal Data from the UK to Other Countries

Should it be necessary for the Cornelius Trust to transfer personal data outside of the UK then the latest guidance from the Information Commissioner’s Office website (www.ico.org.uk) should be sought.

1. Disclosure and Sharing of Personal Information

The Cornelius Trust takes the security and confidentiality of personal data extremely seriously. In certain circumstances, the Cornelius Trust may disclose personal data we hold to third parties. Unless required by law this will not include the sharing of sensitive personal data:

• If we are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation (e.g., for crime or taxation purposes)

• There is a public duty to disclose (e.g., under a UK enactment)

• Disclosure is required to protect the interests of the individual concerned

• For the purpose of seeking legal advice and related proceedings

• The individual concerned has requested (or given their consent to) the data being disclosed (e.g., for the purpose of a confidential reference, or to enable another e.g. another UK-based Christian organisation to provide them with pastoral support)

• In order to enforce or apply any contract with the data subject or other agreements

• To protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction

The Cornelius Trust requires a Confidentiality Agreement Statement to be signed by other UK Military Christian organisations before any data is released. In addition, these organisations MUST have robust data protection policies of their own. Cornelius Trust trustees are required to check their personal data processing arrangements before sharing any personal details. (Template available at Appendix 2).

1. Policy Implementation

Detailed guidance regarding the practical implementation of this policy is available at Appendices 3-4.

1. Changes to this Policy

The Cornelius Trust reserves the right to change this policy at any time, which it keeps under regular review and updates when necessary. Where appropriate, it will notify data subjects of those changes by mail or email.

1. Policy Review

This policy should be reviewed annually.

APPENDIX 1: SUBJECT ACCESS REQUEST FORM

Subject Access Request Form

Under the UK GDPR, you have a right of access to personal information that the Cornelius Trust holds about you.

Completing this form will help us to locate the information you are seeking and deal with your request as quickly as is possible. Alternatively, the same details may be passed orally to us.

Part 1 – About Yourself

Full name:

Current Address:

Previous Address (if relevant):

Phone Number:

Email Address:

Date of Birth:

Part 2 - Locating Your Personal Information

In order for us to be able to locate the information you are seeking, please provide some details, if known, as to where/by whom you feel information is held about you.

Data Details:

(e.g., what type of data, any dates, where and how might be held).

Name of Persons Holding Requested Details:

Any Additional Information:

(Please continue on a separate piece of paper if necessary)

APPENDIX 2: Cornelius Trust Confidentiality Agreement Statement

Cornelius Trust Data Protection Policy

I have read the Cornelius Trust Data Protection Policy and will protect the data shared with me in accordance with Cornelius Trust policy.

Disclosure to other Organisations

The Cornelius Trust will not pass personal data to other third parties. This means the Cornelius Trust will not sell/ exchange its data to/with other organisations.

Disclosing Data for Other Reasons

In certain circumstances the Data Protection Act 2018 allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. There are also circumstances where the law allows Cornelius Trust to disclose data (including sensitive data) without the data subject's consent.

These are:

• Carrying out a legal duty or as authorised by the Secretary of State

• Protecting vital interests of an Individual /Service User or other person

• The Individual/Service User has already made the information public

• Conducting any legal proceedings, obtaining legal advice, or defending any legal rights

• Monitoring for equal opportunities purposes – i.e. race, disability or religion

• Providing a confidential service where the Individual/Service User's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill Individuals/Service Users to provide consent signatures

Correct Processing of Personal Data

The Cornelius Trust regards the lawful and correct treatment of personal information as very important to our successful working, and to maintaining the confidence of those with whom we deal. Under these circumstances the Cornelius Trust will disclose requested data. However, the DPO will ensure the request is legitimate, seeking advice from the board and legal advice where necessary.

Signed:

Name:

Dated:

APPENDIX 3: General Staff Guidelines

General Principles for Policy Implementation

The only people able to access data covered by this policy should be those who need it for performance of their roles within the Cornelius Trust.

• Staff should keep all data secure, by taking sensible precautions following the guidelines below:

• Strong passwords must be used on computers. These should not be shared

• Personal data should not be disclosed to unauthorised people. This includes giving a member's address/email/telephone number

• Data should be regularly reviewed and updated if it is found to be out of date. If it is no longer required, it should be deleted and disposed of

• Staff should request help from the DPO if they are unsure about any aspect of data protection

• When using Email distribution lists, send blind copies

Data Storage

Data Stored on Paper

When data is stored on paper it should be kept in a secure, locked place or container accessible only by authorised personnel on a strictly need to access basis in direct connection with their Cornelius Trust duties.

The following guidelines should be followed by all staff with access to data:

• When not required the paper or files should be kept in a closed opaque file or filing cabinet

• Paper and printouts should not be left where unauthorised people could see them

• Papers containing data should be shredded and disposed of securely when no longer required

Data Stored Electronically

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts, including through the following measures:

• It must be protected by strong passwords

• If it is stored on removeable media (like DVD, USB), these must be kept securely and put away in a secure, lockable storage with only limited authorised access when not in use

• Data should be stored only on designated drivers and servers and should only be uploaded to an approved cloud computing service such as MS Teams which subscribe to UK data protection legislation requirements

• Data should be backed up regularly

• All servers and computers containing data should be protected by an approved security software and a firewall

• Data should be held in as few places as necessary

Personal Data

The Cornelius Trust is routinely required to hold the following personal data where relevant:

• Name, home and work address and telephone numbers

• Email address

• Service number and rank

• Date of birth

• Date of joining

• Bank details

Sensitive Personal Data

Sensitive personal data is information relating to a living individual who can be identified from the data which includes an expression of opinion about the individual.

Exceptionally the Cornelius Trust may hold the following sensitive personal data to fulfil its role effectively (e.g. pertaining to a staff member. Under UK GDPR Sensitive Personal Data is defined as information consisting of:

• religious or philosophical beliefs

In order to process these types of data, consent from the data subject must be obtained by the Cornelius Trust when handling the data. Explicit consent must be given when it is sensitive personal data.

APPENDIX 4: Data Protection Checklist for Staff and Trustees?

Existing Data

• Are you currently holding any personal data?

• Is it held securely?

• For what purpose are you holding it?

• Is it sensitive personal data? Do you have permission from the subject to hold it?

• Does the individual know you are holding their personal data/ have they given their consent?

• Has the Cornelius Trust notified the Data Protection Commissioner that it holds this data and the purpose for which it is held?

• Is the data accurate?

• Does the data still need to be held?

New Data

• Make sure you include reference to the Cornelius Trust Data Protection Policy on the form together with a relevant opt out for other communications

• When collecting data from new contacts by phone, email, or letter, make sure that they know about our data protection statement and email statement

• When requesting a new page to be put on the website that will result in the collection of data ensure that the page contains a link to the Cornelius Trust's Privacy Statement, Data Protection Policy

• Delete the data when it is no longer required

• Do not take personal data from another organisation without the consent of the individual concerned

Using Data

• Are you passing personal data to anyone else?

• Inside the Cornelius Trust

• Outside the Cornelius Trust

• Are you using blind copies when sending email distribution lists?

• Is there a confidentiality agreement in place where it is necessary to pass data to a permitted third party?

• Do not pass personal data to any person outside of the Cornelius Trust without the permission of the individual