LOWESTOFT COMMUNITY CHURCH (LCC)
PRIVACY POLICY

CONTENTS

Legislation

This policy is intended to meet the requirements of the Data Protection Act 2018 as amended (DPA 2018) and the UK General Data Protection Regulation (UKGDPR), which came into effect on 1 January 2021 and sets out the key principles, rights and obligations for most processing of personal data in the UK.

It is based on guidance published by the Information Commissioner's Office (ICO) on the UKGDPR and by its adoption, LCC aims to ensure that personal data about staff, members, volunteers, foodbank and debt counselling clients, visitors and other individuals is collected, stored and processed in accordance with the legislation. It applies to all personal data, regardless of whether it is in electronic format or on paper and filed in an organised way.

Data protection is the fair and proper use of information about people. Personal data means information about a particular living individual and may include the person's:

- Name (including initials)
- Identification number
- Location data
- Online identifier, such as a username

It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

The legislation stipulates special categories of personal data, which is more sensitive and so needs more protection, and this includes information about an individual's religious beliefs.

Complying with the UKGDPR requires LCC to be proactive and organised in its approach to data protection; demonstrating that compliance requires LCC to evidence the action taken. Specifically:

Article 24(1) of the UKGDPR requires LCC to:

- implement technical and organisational measures to ensure, and demonstrate, compliance
- implement measures that are risk-based and proportionate
- review and update those measures as necessary

Article 30 of the UKGDPR requires LCC to document:

- Its name and contact details
- The purposes of its processing
- A description of the categories of individuals and categories of personal data
- The categories of recipients of personal data
- Retention schedules
- A description of its technical and organisational security measures

As membership of LCC reveals an individual's religious belief, LCC is involved in the processing of what the UKGDPR designates as a special category of data and therefore cannot take advantage of the limited exemption that otherwise absolves a small organisation from having to document its processing activities.

Thus, LCC's fundamental approach is to:

- Ensure a good understanding and awareness of data protection within its organisation
- Implement comprehensive, but proportionate, policies/procedures for handling personal data
- Keep records of what it does and why

Data Protection Principles

The data protection principles enshrined in the UKGDPR, with which LCC must comply, state that personal data must be:

- Processed lawfully, fairly and in a transparent manner (i.e. the individual knows why their data is held, what will be done with it and for how long it will be kept)
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how LCC aims to follow these principles.

Data Protection by Design and Default

This concept is expressed by the UKGDPR and basically requires LCC to implement the data protection principles effectively by adopting appropriate technical and organisational measures and integrating safeguards into its processing that protect individual rights.

In compliance with Article 25 of the UKGDPR, LCC will put measures in place to show that it has integrated data protection into all its data processing activities, including:

- Ensuring that its Trustees, staff and relevant volunteers maintain an adequate and current understanding of LCC's data protection obligations
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles enshrined in the legislation
- Completing Data Protection Impact Assessments where LCC's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies
- Integrating data protection into internal documents including this policy, any related policies and Privacy Notices
- Regularly training members of staff (and those volunteering in roles that gives them access to personal data) on data protection law, this policy and any other data protection matters, keeping a record of the delivery of such training
- Regularly conducting reviews and audits to provide assurance that LCC continues to meet its data protection obligations
- Maintaining records of LCC's personal data processing activities, such as:
    - For the benefit of data subjects, providing Privacy Notices as required by data protection legislation that contain all the information that LCC is required to share about how it uses and processes their personal data
    - Details of the type of data, the data subject, how and why LCC is using and storing the data, retention periods, the measure to keep the data secure and any third-party recipients

LCC will be guided in its choice of measures and safeguards by applying the 'checklists' provided on the ICO's website, as appropriate. These are reproduced as **Appendices 1 to 10** to this policy.

Data Controller

LCC determines the purposes and the means of processing of personal data relating to staff, members, volunteers, foodbank and debt counselling clients, visitors and other individuals and is therefore a data controller under the UKGDPR. Such processing includes collecting, recording, storing, using, analysing, combining, disclosing or deleting this data.

LCC is registered as a Data Controller with the ICO and will renew this registration annually or as otherwise legally required.

Roles and Responsibilities

The Trustees have overall responsibility for ensuring that LCC complies with the requirements of the UKGDPR and that it has the necessary staff and skills to do so. Accordingly, by this policy, they aim to build a culture of data security awareness within LCC.

Whilst the UKGDPR does not oblige LCC to appoint a formal Data Protection Officer (because its processing of special category data is not on "*a large scale*"), it nevertheless expects someone to be identified who has day-to-day responsibility for data security. LCC gives that responsibility to the Lead Elder.

This policy applies to all staff employed by LCC and to those volunteering in roles that gives them access to personal data. It also applies to external organisations or individuals working on LCC's behalf.

Staff and relevant volunteers must only process personal data where it is necessary to do their jobs or fulfill their role and they are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Deleting or anonymizing personal data they hold when it is no longer needed
- Informing LCC of any changes to their own personal data, such as a change of address
- Notifying and/or seeking guidance from the LCC Lead Elder or the Trustees if:
    - They are unsure about the operation of this policy or their legal obligations concerning personal data security
    - They are concerned that this policy is not being followed
    - They are not certain that they have a lawful basis to use personal data in a particular way
    - They need to rely on or capture an individual's consent
    - There has been a personal data breach
    - They are engaging in a new activity that may affect the privacy rights of individuals
    - They need help with any contracts or sharing personal data with third parties

Training

Under the UKGDPR, LCC must ensure that anyone acting under its authority with access to personal data does not process that data unless LCC has instructed them to do so. Hence it is vital that LCC's staff (and those volunteering in roles that gives them access to personal data) understand the importance of protecting personal data, are familiar with LCC's data security measures and adhere to its relevant procedures.

Accordingly, appropriate training is delivered by someone with the necessary skill and knowledge to all staff and relevant volunteers immediately upon their induction, prior to them being given access to personal data. Such training will be refreshed bi-annually (or when significant changes to legislation, guidance or LCC's processes make it necessary) and will include such topics as:

- LCC's responsibilities as a Data Controller under the UKGDPR
- Staff and relevant volunteers' responsibilities for protecting personal data (including the possibility that they may commit criminal offences if they deliberately try to access or disclose this data without authority)
- The dangers of people trying to obtain or alter personal data by deception (e.g. by pretending to be the individual whom the data concerns, or enabling staff to recognise 'phishing' attacks)
- The proper procedures for identifying callers
- Restrictions placed on their personal use of LCC's systems (e.g. to avoid virus infection or spam)

Data Protection Impact Assessments (DPIAs)

As an integral part of data protection by design and by default, LCC will use DPIAs as a tool to identify and minimise the data protection risks of its processing activities. They will help determine the type of technical and organisational measures needed to ensure compliance with the data protection principles in respect of processing that is likely to result in a high risk to individuals, e.g. because it involves special category data.

Each DPIA will adopt the template provided on the ICO website (reproduced at **Appendix 11**), but essentially will:

- Describe the nature, scope, context and purposes of the processing
- Assess necessity, proportionality and compliance measures
- Identify and assess risks to individuals
- Identify any additional measures to mitigate those risks

Collection and Processing of Personal Data

LCC will only collect personal data for specified, explicit and legitimate reasons, which will be explained to the individual when their data is first collected. That individual will be provided with the information that is required by the data protection legislation, in the form of a Privacy Notice (at **Appendix 12**) which is:

- Concise, transparent, intelligible and easily accessible
- Written in clear and plain language, particularly if addressed to a child
- Free of charge.

LCC will only process personal data where it has a lawful basis to do so (i.e. because the processing falls within one of the six categories specified by Article 6 of the UKGDPR). That basis will be one of the following:

- The data needs to be processed so that LCC can fulfil a contract with the individual, or the individual has asked LCC to take specific steps before entering into a contract
- The data needs to be processed for the legitimate interests of LCC or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a child) has freely given clear consent for LCC to process their personal data for a specific purpose
- LCC will determine and evidence its legitimate interests by conducting an assessment in the format provided on the ICO website (reproduced at **Appendix 13**)

When consent is sought and given, it will:

- Involve a positive 'opt-in'
- Offer individuals real choice and control
- Be clear and concise
- Explain how that consent can be withdrawn (and make it easy to do so)

LCC will retain evidence of any consent obtained (detailing the individual and when, how, and what they were told), keep it under review and refresh it if anything changes.

If LCC wants to use personal data for reasons other than those given when it was first obtained, LCC will inform the individuals concerned prior to doing so, and seek consent where necessary.

For special categories of personal data, LCC will also meet one of the special category conditions for processing which are set out in the legislation (see below).

Special Category Data

The UKGDPR definition of special category data includes personal data revealing 'religious or philosophical beliefs'. Personal data concerning LCC's members will fall into this category.

Article 9 of the UKGDPR prohibits the processing of special category data, but specifies ten exceptions to this general prohibition, usually referred to as 'conditions for processing special category data'. Hence, in addition to identifying a lawful basis for its processing of general data under Article 6, LCC must meet one of these ten conditions in Article 9 before it can process the special category data.

LCC considers that its processing of special category data meets one or more of the following Article 9 conditions:

- (a) Explicit consent
- (d) Not-for-profit bodies.

When relying on condition (a), LCC will ensure that explicit consent is confirmed in a clear statement that is separate from any other consent being sought and specifies the nature of the special category data.

When relying on condition (d), LCC will:

- Only process special category data as part of its legitimate activities, i.e. those that fall within the purposes and powers set out in its constitution and are not unlawful or unethical in any way
- Limit such processing to the data of members, former members, or other individuals in regular contact with LCC in connection with its purposes
- Have appropriate safeguards in place
- Not disclose the data to a third party without the individual's explicit consent

Data Security and Storage of Records

Article 5(1)(f) of the UK GDPR requires personal data to be:

"Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures".

Accordingly, to prevent the personal data it holds being accidentally or deliberately compromised, LCC will implement security measures that seek to ensure that the data:

- Is kept safe from unauthorised, unlawful or accidental processing, loss, destruction or damage
- Can only be accessed, altered, disclosed or deleted by those that have been authorised to do so (and that those people only act within the scope of the authority given them)
- Is accurate and complete in relation to why it is being processed
- Remains accessible and usable (i.e. if personal data is accidentally lost, altered or destroyed, it can be recovered, thus preventing any damage or distress to the individuals concerned)

To determine what security measures are appropriate, LCC will assess its information risk by reviewing the personal data held and the way it is used, thereby identifying how valuable, sensitive or confidential it is and what damage or distress might be caused if it was compromised. This process will be documented as an Information Audit (in the format at **Appendix 14**), repeated annually (and when significant change occurs) and take account of factors such as:

- The nature and extent of LCC's premises and computer systems and how the access given to them is controlled (including for maintenance)
- The quality of doors and locks on the premises and the protection afforded by alarms, security lighting or CCTV
- The supervision of visitors to LCC's premises
- The methods of disposal of any paper and electronic waste
- The methods of keeping IT equipment, particularly mobile devices, secure
- The security of LCC's network and IT systems, including the effectiveness of access controls
- Online security (e.g. security of LCC website and any other online service or application)
- Staff and volunteer numbers and the extent of their access to personal data
- The incidence of staff working from home
- Coordination between key staff (e.g. when IT equipment is acquired or discarded)
- Any personal data held or used by a data processor acting on LCC's behalf

With regard to the security of LCC's IT systems, this assessment of information risk will be guided by the document published by the ICO entitled "*A practical guide to IT security - Ideal for the small business*", which appears on its website.

In compliance with the UKGDPR's requirements, LCC will establish a process for regularly testing and evaluating the effectiveness of its security measures. Such testing will be appropriate to the nature of the processing and the data, but will include 'stress tests' of LCC's network and IT systems that are designed to reveal areas of potential risk and things that can be improved.

LCC's security measures will include:

- Proper procedures to identify callers
- Papers containing confidential personal data are not left on office desks or anywhere else where there is general access
- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Personal data in LCC's possession is only stored on electronic devices that are the property of LCC
- Personal data is only taken off LCC's premises if absolutely necessary and on such rare occasions it is not left unattended in cars, or in places where others may have access to it. The person responsible for the data will take appropriate steps to prevent it from being lost or stolen, will return it to LCC's premises at the earliest opportunity and will sign it in/out in a central record maintained for this purpose
- Passwords that are at least 8 characters long containing letters and numbers are used to access LCC's computers, laptops and other electronic devices. Those using such devices are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices

Clear Desk Policy

In compliance with the UKGDPR, which requires personal data to be held securely at all times, LCC operates a clear desk policy for all staff and relevant volunteers. This reduces the threat of a security breach as confidential information is locked away or otherwise securely stored.

At the end of each working day or when the workplace is vacated for an extended period during the day, all work-related paperwork and removable storage media (especially anything containing personal data) must be placed into secure storage (e.g. locked desk drawer, filing cabinet or cupboard).

Paperwork that is needed should be acted upon and then appropriately filed, whilst that which is unwanted containing personal data or sensitive information must be disposed of.
Staff and relevant volunteers should not print out hard copies of e-mails or documents just to read them unless this is vital. Anything printed should be collected from the printer immediately, particularly if the document contains personal data.

Disposal of Records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where LCC cannot or does not need to rectify or update it.

For example, paper-based records will be shredded and electronic files overwritten or deleted. If a third party is used to safely dispose of records on LCC's behalf, that third party will be required to provide sufficient guarantees that it complies with data protection law.

LCC keeps a record of any data that has been securely destroyed.

Sharing of Personal Data

LCC will not normally share personal data with anyone else, but may do so where:

- There is a need to liaise with other agencies, such as those that LCC partners with (when prior consent will be obtained)
- LCC's suppliers or contractors need data to enable LCC to provide services to its staff, members and others – for example, IT companies. When doing this, LCC will:
    - Only appoint suppliers or contractors who can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor to ensure the fair and lawful processing of any personal data LCC shares
    - Only share data that the supplier or contractor needs to carry out their service

Where LCC does need to share personal data with a third party, it carries out due diligence and takes reasonable steps to ensure it is stored securely and is adequately protected.

LCC will also share personal data with law enforcement and government bodies where it is legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- Legal proceedings
- The discharge of LCC's safeguarding obligations

LCC may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of LCC's members or staff.

If LCC were to transfer personal data to a country or territory outside the European Economic Area, it would do so in accordance with data protection law.

Use of Email

LCC provides designated members of staff with their own email account as a work-based tool. This work email account must be used for all LCC business in accordance with LCC's ICT Policy and, to guard against personal data breaches, such use is subject to the following rules:

- It is the responsibility of each account holder to keep their password(s) secure
- The email account must be checked regularly and all received emails must be responded to promptly
- All emails created or received must be subjected to frequent house-keeping and those of short-term value promptly deleted
- Recipients of sent emails, particularly those being copied in, must be appropriately targeted, carefully identified and kept to the minimum necessary. The facility to hide the names of recipients copied in will be utilised, unless there is a legitimate reason for not doing so
- Attachments to emails from untrusted sources must never be opened
- Email attachments must not be sent or forwarded unnecessarily
- The email account must not be used to store attachments; they should be saved to the appropriate shared drive/folder
- When personal data is being sent by email, because it cannot be transmitted by other secure means, it must be encrypted and the following procedure must be adopted with caution before the email is sent:

    - The details, including accurate email address, of any intended recipient of the information are to be independently verified
    - The email is not to be copied or forwarded to more recipients than is absolutely necessary
    - The information is to be sent as an encrypted/password protected document and the encryption key or password is to be provided by a separate contact with the recipient(s) – preferably by telephone
    - The name of the relevant individual(s) is not to be identified in the email subject line
    - "CONFIDENTIAL" is to be put in the subject line and as a header in the email and any attachments to it
    - Confirmation of safe receipt is to be requested

Photographs and Videos

As part of its activities, LCC may take photographs and record images of individuals participating in those activities.

LCC will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. LCC will clearly explain how the photograph and/or video will be used to both the parent/carer and child.

Where LCC does not need parental consent, it will clearly explain to the individual how the photograph and/or video will be used.

Uses may include:

- On LCC's website or on display boards within its premises
- Outside of LCC by external agencies such as the local or national press.

When using photographs and videos, LCC will not accompany them with any personal information about the individual, to ensure they cannot be identified.

Consent can be refused or withdrawn at any time. If consent is withdrawn, LCC will delete the photograph or video and not distribute it further.

Personal Data Breaches

LCC will take appropriate measures against unauthorised or unlawful processing, disclosure, loss, destruction or alteration of personal data and thus endeavour to ensure that there are no personal data breaches.

Such breaches may include, or result from the following:

- Safeguarding information being made available to an unauthorised person
- The loss or theft of personal data
- The loss or theft of an LCC laptop or similar device containing non-encrypted personal data
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Unforeseen circumstances such as a fire or flood
- Human error
- Hacking attacks
- 'Blagging' offences (where information is obtained by deception)

In the unlikely event of a suspected data breach, LCC will follow the procedure set out in **Appendix 15,** which may involve the matter being reported to the ICO within a set time limit.

Subject Access Requests

Individuals have a right to make a 'subject access request' to gain access to personal information that LCC holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

When responding to requests, LCC:

- May ask the individual to provide 2 forms of identification
- Will respond without delay and within 1 month of receipt of the request unless the request is complex or numerous. In such instances, the individual will be told within 1 month that LCC will comply within 3 months of receipt of the request and provided with an explanation for why the extension is necessary

If the request is unfounded or excessive, LCC may refuse to act on it, or charge a reasonable fee which takes account of administrative costs. A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information. When LCC refuses a request, it will tell the individual why, and tell them they have the right to complain to the ICO.

Other Data Protection Rights of the Individual

In addition to the right to make a subject access request and to receive information when LCC is collecting their data about how LCC uses and processes it, individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask LCC to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO.

Approved & adopted by LCC Trustees:

	Approved	**Reviewed and amended**	**Reviewed**	**Reviewed**
Date	March 2021	January 2024		
Signed	REDACTED	REDACTED		

Appendix 1

Lawfulness and Lawful basis for processing checklists from ICO website

Lawfulness:

☐ We have identified an appropriate lawful basis (or bases) for our processing.

☐ If we are processing special category data or criminal offence data, we have identified a condition for processing this type of data.

☐ We don't do anything generally unlawful with personal data.

Fairness:

☐ We have considered how the processing may affect the individuals concerned and can justify any adverse impact.

☐ We only handle people's data in ways they would reasonably expect, or we can explain why any unexpected processing is justified.

☐ We do not deceive or mislead people when we collect their personal data.

Transparency:

☐ We are open and honest and comply with the transparency obligations of the right to be informed.

Purpose limitation:

☐ We have clearly identified our purpose or purposes for processing.

☐ We have documented those purposes.

☐ We include details of our purposes in our privacy information for individuals.

☐ We regularly review our processing and, where necessary, update our documentation and our privacy information for individuals.

☐ If we plan to use personal data for a new purpose other than a legal obligation or function set out in law, we check that this is compatible with our original purpose or we get specific consent for the new purpose.

Data minimisation:

☐ We only collect personal data we actually need for our specified purposes.

☐ We have sufficient personal data to properly fulfil those purposes.

☐ We periodically review the data we hold and delete anything we don't need.

Accuracy:

☐ We ensure the accuracy of any personal data we create.

☐ We have appropriate processes in place to check the accuracy of the data we collect, and we record the source of that data.

☐ We have a process in place to identify when we need to keep the data updated to properly fulfil our purpose, and we update it as necessary.

☐ If we need to keep a record of a mistake, we clearly identify it as a mistake.

☐ Our records clearly identify any matters of opinion, and where appropriate whose opinion it is and any relevant changes to the underlying facts.

☐ We comply with the individual's right to rectification and carefully consider any challenges to the accuracy of the personal data.

☐ As a matter of good practice, we keep a note of any challenges to the accuracy of the personal data.

Storage limitation:

☐ We know what personal data we hold and why we need it.

☐ We carefully consider and can justify how long we keep personal data.

☐ We have a policy with standard retention periods where possible, in line with documentation obligations.

☐ We regularly review our information and erase or anonymise personal data when we no longer need it.

☐ We have appropriate processes in place to comply with individuals' requests for erasure under 'the right to be forgotten'.

☐ We clearly identify any personal data that we need to keep for public interest archiving, scientific or historical research, or statistical purposes.

Lawful basis for processing:

☐ We have reviewed the purposes of our processing activities and selected the most appropriate lawful basis (or bases) for each activity.

☐ We have checked that the processing is necessary for the relevant purpose and are satisfied that there is no other reasonable and less-intrusive way to achieve that purpose.

☐ We have documented our decision on which lawful basis applies to help us demonstrate compliance.

☐ We have included information about both the purposes of the processing and the lawful basis for the processing in our privacy notice.

☐ Where we process special category data, we have also identified a condition for processing special category data and have documented this.

Appendix 2

Consent checklists from ICO website

Asking for consent:

☐ We have checked that consent is the most appropriate lawful basis for processing.
☐ We have made the request for consent prominent and separate from our terms and conditions.
☐ We ask people to positively opt in.
☐ We don't use pre-ticked boxes or any other type of default consent.
☐ We use clear, plain language that is easy to understand.
☐ We specify why we want the data and what we're going to do with it.
☐ We give separate distinct ('granular') options to consent separately to different purposes and types of processing.
☐ We name our organisation and any third party controllers who will be relying on the consent.
☐ We tell individuals they can withdraw their consent.
☐ We ensure that individuals can refuse to consent without detriment.
☐ We avoid making consent a precondition of a service.
☐ If we offer online services directly to children, we only seek consent if we have age-verification measures (and parental-consent measures for younger children) in place.

Recording consent:

☐ We keep a record of when and how we got consent from the individual.
☐ We keep a record of exactly what they were told at the time.

Managing consent:

☐ We regularly review consents to check that the relationship, the processing and the purposes have not changed.
☐ We have processes in place to refresh consent at appropriate intervals, including any parental consents.
☐ We make it easy for individuals to withdraw their consent at any time and publicise how to do so.
☐ We act on withdrawals of consent as soon as we can.
☐ We don't penalise individuals who wish to withdraw consent.

Appendix 3

Legitimate interests and Special Category Data checklists from ICO website

Legitimate interests:

☐ We have checked that legitimate interests is the most appropriate basis.

☐ We understand our responsibility to protect the individual's interests.

☐ We have conducted a legitimate interests assessment (LIA) and kept a record of it, to ensure that we can justify our decision.

☐ We have identified the relevant legitimate interests.

☐ We have checked that the processing is necessary and there is no less intrusive way to achieve the same result.

☐ We have done a balancing test and are confident that the individual's interests do not override those legitimate interests.

☐ We only use individuals' data in ways they would reasonably expect, unless we have a very good reason.

☐ We are not using people's data in ways they would find intrusive or which could cause them harm, unless we have a very good reason.

☐ If we process children's data, we take extra care to make sure we protect their interests.

☐ We have considered safeguards to reduce the impact where possible.

☐ We have considered whether we can offer an opt out.

☐ If our LIA identifies a significant privacy impact, we have considered whether we also need to conduct a DPIA.

☐ We keep our LIA under review and repeat it if circumstances change.

☐ We include information about our legitimate interests in our privacy information.

Special Category Data:

☐ We have checked the processing of the special category data is necessary for the purpose we have identified and are satisfied there is no other reasonable and less intrusive way to achieve that purpose.

☐ We have identified an Article 6 lawful basis for processing the special category data.

☐ We have identified an appropriate Article 9 condition for processing the special category data.

☐ We have documented which special categories of data we are processing.

☐ Where required, we have an appropriate policy document in place.

☐ We have considered whether we need to do a DPIA.

☐ We include specific information about our processing of special category data in our privacy information for individuals.

☐ We have considered whether the risks associated with our use of special category data affect our other obligations around data minimisation, security, and appointing Data Protection Officers (DPOs) and representatives.

Appendix 4

Right to be informed checklists from ICO website

What to provide:

We provide individuals with all the following privacy information:

☐ The name and contact details of our organisation.

☐ The name and contact details of our representative (if applicable).

☐ The contact details of our data protection officer (if applicable).

☐ The purposes of the processing.

☐ The lawful basis for the processing.

☐ The legitimate interests for the processing (if applicable).

☐ The categories of personal data obtained (if the personal data is not obtained from the individual it relates to).

☐ The recipients or categories of recipients of the personal data.

☐ The details of transfers of the personal data to any third countries or international organisations (if applicable).

☐ The retention periods for the personal data.

☐ The rights available to individuals in respect of the processing.

☐ The right to withdraw consent (if applicable).

☐ The right to lodge a complaint with a supervisory authority.

☐ The source of the personal data (if the personal data is not obtained from the individual it relates to).

☐ The details of whether individuals are under a statutory or contractual obligation to provide the personal data (if applicable, and if the personal data is collected from the individual it relates to).

☐ The details of the existence of automated decision-making, including profiling (if applicable).

When to provide it:

☐ We provide individuals with privacy information at the time we collect their personal data from them.

If we obtain personal data from a source other than the individual it relates to, we provide them with privacy information:

☐ within a reasonable of period of obtaining the personal data and no later than one month;

☐ if we plan to communicate with the individual, at the latest, when the first communication takes place; or

☐ if we plan to disclose the data to someone else, at the latest, when the data is disclosed.

How to provide it:

We provide the information in a way that is:

☐ Concise;
☐ Transparent;
☐ Intelligible;
☐ Easily accessible; and
☐ Uses clear and plain language.

Changes to the information:

☐ We regularly review and, where necessary, update our privacy information.
☐ If we plan to use personal data for a new purpose, we update our privacy information and communicate the changes to individuals before starting any new processing.

Best practice – drafting the information:

☐ We undertake an information audit to find out what personal data we hold and what we do with it.
☐ We put ourselves in the position of the people we're collecting information about.
☐ We carry out user testing to evaluate how effective our privacy information is.

Best practice – delivering the information:

When providing our privacy information to individuals, we use a combination of appropriate techniques, such as:

☐ A layered approach;
☐ Dashboards;
☐ Just-in-time notices;
☐ Icons; and
☐ Mobile and smart device functionalities.

Appendix 5

Subject Access Requests checklists from ICO website

Preparing for subject access requests:

☐ We know how to recognise a subject access request and we understand when the right of access applies.

☐ We have a policy for how to record requests we receive verbally.

☐ We understand what steps we need to take to verify the identity of the requester, if necessary.

☐ We understand when we can pause the time limit for responding if we need to ask for clarification.

☐ We understand when we can refuse a request and are aware of the information we need to provide to individuals when we do so.

☐ We understand the nature of the supplementary information we need to provide in response to a subject access request.

☐ We have suitable information management systems in place to allow us to locate and retrieve information efficiently.

Complying with subject access requests:

☐ We have processes in place to ensure that we respond to a subject access request without undue delay and within one month of receipt.

☐ We understand how to perform a reasonable search for the information.

☐ We understand what we need to consider if a third party makes a request on behalf of an individual.

☐ We are aware of the circumstances in which we can extend the time limit to respond to a request.

☐ We understand how to assess whether a child is mature enough to understand their rights.

☐ We understand that there is a particular emphasis on using clear and plain language if we are disclosing information to a child.

☐ We understand what we need to consider if a request includes information about others.

☐ We are able to deliver the information securely to an individual, and in the correct format.

Appendix 6

Accountability, Governance and Security checklists from ICO website

Accountability and governance:

☐ We take responsibility for complying with the UK GDPR, at the highest management level and throughout our organisation.

☐ We keep evidence of the steps we take to comply with the UK GDPR.

We put in place appropriate technical and organisational measures, such as:

☐ Adopting and implementing data protection policies (where proportionate);

☐ Taking a 'data protection by design and default' approach - putting appropriate data protection measures in place throughout the entire lifecycle of our processing operations;

☐ Putting written contracts in place with organisations that process personal data on our behalf;

☐ Maintaining documentation of our processing activities;

☐ Implementing appropriate security measures;

☐ Recording and, where necessary, reporting personal data breaches;

☐ Carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests;

☐ Appointing a data protection officer (where necessary); and

☐ Adhering to relevant codes of conduct and signing up to certification schemes (where possible).

☐ We review and update our accountability measures at appropriate intervals.

Security:

☐ We undertake an analysis of the risks presented by our processing and use this to assess the appropriate level of security we need to put in place.

☐ When deciding what measures to implement, we take account of the state of the art and costs of implementation.

☐ We have an information security policy (or equivalent) and take steps to make sure the policy is implemented.

☐ Where necessary, we have additional policies and ensure that controls are in place to enforce them.

☐ We make sure that we regularly review our information security policies and measures and, where necessary, improve them.

☐ We have assessed what we need to do by considering the security outcomes we want to achieve.

☐ We have put in place basic technical controls such as those specified by established frameworks like Cyber Essentials.

☐ We understand that we may also need to put other technical measures in place depending on our circumstances and the type of personal data we process.

☐ We use encryption and/or pseudonymisation where it is appropriate to do so.

☐ We understand the requirements of confidentiality, integrity and availability for the personal data we process.

☐ We make sure that we can restore access to personal data in the event of any incidents, such as by establishing an appropriate backup process.

☐ We conduct regular testing and reviews of our measures to ensure they remain effective, and act on the results of those tests where they highlight areas for improvement.

☐ Where appropriate, we implement measures that adhere to an approved code of conduct or certification mechanism.

☐ We ensure that any data processor we use also implements appropriate technical and organisational measures.

Appendix 7

Documentation checklists from ICO website

Documentation of processing activities – requirements:

☐ If we are a controller for the personal data we process, we document all the applicable information under Article 30(1) of the UK GDPR.

☐ If we are a processor for the personal data we process, we document all the applicable information under Article 30(2) of the UK GDPR.

☐ We document our processing activities in writing.

☐ We document our processing activities in a granular way with meaningful links between the different pieces of information.

☐ We conduct regular reviews of the personal data we process and update our documentation accordingly.

Documentation of processing activities – best practice:

When preparing to document our processing activities we:

☐ Do information audits to find out what personal data our organisation holds;

☐ Distribute questionnaires and talk to staff across the organisation to get a more complete picture of our processing activities; and

☐ Review our policies, procedures, contracts and agreements to address areas such as retention, security and data sharing.

As part of our record of processing activities we document, or link to documentation, on:

☐ Information required for privacy notices;

☐ Records of consent;

☐ Controller-processor contracts;

☐ The location of personal data;

☐ Data Protection Impact Assessment reports; and

☐ Records of personal data breaches.

☐ We document our processing activities in electronic form so we can add, remove and amend information easily.

Appendix 8

Data protection by design and default checklist from ICO website

☐ We consider data protection issues as part of the design and implementation of systems, services, products and business practices.

☐ We make data protection an essential component of the core functionality of our processing systems and services.

☐ We anticipate risks and privacy-invasive events before they occur and take steps to prevent harm to individuals.

☐ We only process the personal data that we need for our purposes(s), and that we only use the data for those purposes.

☐ We ensure that personal data is automatically protected in any IT system, service, product, and/or business practice, so that individuals should not have to take any specific action to protect their privacy.

☐ We provide the identity and contact information of those responsible for data protection both within our organisation and to individuals.

☐ We adopt a 'plain language' policy for any public documents so that individuals easily understand what we are doing with their personal data.

☐ We provide individuals with tools so they can determine how we are using their personal data, and whether our policies are being properly enforced.

☐ We offer strong privacy defaults, user-friendly options and controls, and respect user preferences.

☐ We only use data processors that provide sufficient guarantees of their technical and organisational measures for data protection by design.

☐ When we use other systems, services or products in our processing activities, we make sure that we only use those whose designers and manufacturers take data protection issues into account.

☐ We use privacy-enhancing technologies (PETs) to assist us in complying with our data protection by design obligations.

Appendix 9

Data Protection Impact Assessments (DPIAs) checklists from ICO website

DPIA awareness checklist:

☐ We provide training so that our staff understand the need to consider a DPIA at the early stages of any plan involving personal data.

☐ Our existing policies, processes and procedures include references to DPIA requirements.

☐ We understand the types of processing that require a DPIA and use the screening checklist to identify the need for a DPIA, where necessary.

☐ We have created and documented a DPIA process.

☐ We provide training for relevant staff on how to carry out a DPIA.

DPIA screening checklist:

☐ We consider carrying out a DPIA in any major project involving the use of personal data.

☐ We consider whether to do a DPIA if we plan to carry out any other:

☐ Evaluation or scoring;

☐ Automated decision-making with significant effects;

☐ Systematic monitoring;

☐ Processing of sensitive data or data of a highly personal nature;

☐ Processing on a large scale;

☐ Processing of data concerning vulnerable data subjects;

☐ Innovative technological or organisational solutions;

☐ Processing that involves preventing data subjects from exercising a right or using a service or contract.

☐ We always carry out a DPIA if we plan to:

☐ Use systematic and extensive profiling or automated decision-making to make significant decisions about people;

☐ Process special-category data or criminal-offence data on a large scale;

☐ Systematically monitor a publicly accessible place on a large scale;

☐ Use innovative technology in combination with any of the criteria in the European guidelines;

☐ Use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit;

☐ Carry out profiling on a large scale;

☐ Process biometric or genetic data in combination with any of the criteria in the European guidelines;

☐ Combine, compare or match data from multiple sources;

☐ Process personal data without providing a privacy notice directly to the individual in combination with any of the criteria in the European guidelines;

☐ Process personal data in a way that involves tracking individuals' online or offline location or behaviour, in combination with any of the criteria in the European guidelines;

☐ Process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them;

☐ Process personal data that could result in a risk of physical harm in the event of a security breach.

☐ We carry out a new DPIA if there is a change to the nature, scope, context or purposes of our processing.

☐ If we decide not to carry out a DPIA, we document our reasons.

DPIA process checklist:

☐ We describe the nature, scope, context and purposes of the processing.

☐ We ask our data processors to help us understand and document their processing activities and identify any associated risks.

☐ We consider how best to consult individuals (or their representatives) and other relevant stakeholders.

☐ We ask for the advice of our data protection officer.

☐ We check that the processing is necessary for and proportionate to our purposes, and describe how we will ensure compliance with data protection principles.

☐ We do an objective assessment of the likelihood and severity of any risks to individuals' rights and interests.

☐ We identify measures we can put in place to eliminate or reduce high risks.

☐ We record our decision-making in the outcome of the DPIA, including any difference of opinion with our DPO or individuals consulted.

☐ We implement the measures we identified, and integrate them into our project plan.

☐ We consult the ICO before processing, if we cannot mitigate high risks.

☐ We keep our DPIAs under review and revisit them when necessary.

Have we written a good DPIA?

Within our DPIA, we have:

☐ Confirmed whether the DPIA is a review of pre-GDPR processing or covers intended processing, including timelines in either case;

☐ Explained why we needed a DPIA, detailing the types of intended processing that made it a requirement;

☐ Structured the document clearly, systematically and logically;

☐ Written the DPIA in plain English, with a non-specialist audience in mind, explaining any technical terms and acronyms we have used;

☐ Set out clearly the relationships between controllers, processors, data subjects and systems, using both text and data-flow diagrams where appropriate;

☐ Ensured that the specifics of any flows of personal data between people, systems, organisations and countries have been clearly explained and presented;

☐ Explicitly stated how we are complying with each of the Data Protection Principles under GDPR and clearly explained our lawful basis for processing (and special category conditions if relevant);

☐ Explained how we plan to support the relevant information rights of our data subjects;

☐ Identified all relevant risks to individuals' rights and freedoms, assessed their likelihood and severity, and detailed all relevant mitigations;

☐ Explained sufficiently how any proposed mitigation reduces the identified risk in question;

☐ Evidenced our consideration of any less risky alternatives to achieving the same purposes of the processing, and why we didn't choose them;

☐ Given details of stakeholder consultation (e.g. data subjects, representative bodies) and included summaries of findings;

☐ Attached any relevant additional documents we reference in our DPIA, e.g. Privacy Notices, consent documents;

☐ Recorded the advice and recommendations of our DPO (where relevant) and ensured the DPIA is signed off by the appropriate people;

☐ Agreed and documented a schedule for reviewing the DPIA regularly or when we change the nature, scope, context or purposes of the processing;

☐ Consulted the ICO if there are residual high risks we cannot mitigate.

Appendix 10

Personal Data Breaches checklists from ICO website

Preparing for a personal data breach:

☐ We know how to recognise a personal data breach.

☐ We understand that a personal data breach isn't only about loss or theft of personal data.

☐ We have prepared a response plan for addressing any personal data breaches that occur.

☐ We have allocated responsibility for managing breaches to a dedicated person or team.

☐ Our staff know how to escalate a security incident to the appropriate person or team in our organisation to determine whether a breach has occurred.

Responding to a personal data breach:

☐ We have in place a process to assess the likely risk to individuals as a result of a breach.

☐ We have a process to inform affected individuals about a breach when their rights and freedoms are at high risk.

☐ We know we must inform affected individuals without undue delay.

☐ We know who is the relevant supervisory authority for our processing activities.

☐ We have a process to notify the ICO of a breach within 72 hours of becoming aware of it, even if we do not have all the details yet.

☐ We know what information we must give the ICO about a breach.

☐ We know what information about a breach we must provide to individuals, and that we should provide advice to help them protect themselves from its effects.

☐ We document all breaches, even if they don't all need to be reported.

Appendix 11

Data Protection Impact Assessment (DPIA) Template from ICO website

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?
Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?
Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no

Step 7: Sign off and record outcomes

Item	Name/Position/Date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA

Appendix 12

Lowestoft Community Church Privacy Notice

This notice sets out how we, Lowestoft Community Church CIO, will process any personal information we collect from you or that you provide to us.

We will collect and process your personal information in accordance with the Data Protection Act 2018 (the Act), and the United Kingdom General Data Protection Regulation (UKGDPR). For the purpose of the Act, we are the Data Controller of personal data we hold about you.

Our contact details

Lowestoft Community Church CIO
Address:
The Depot, 8 Hadenham Road, South Lowestoft Industrial Estate, Lowestoft, Suffolk. NR33 7NF
Telephone: 01502 537527
Email: bparish@lcc-lowestoft.co.uk

Due to our status, the UKGDPR does not oblige us to appoint a formal Data Protection Officer. However, we have given day-to-day responsibility for data protection matters to Ben Parish (Lead Elder) and therefore any related enquiries should be directed to him.

The type of personal information we collect about you

We currently collect and process the following information:

- Your contact details
- Your attendance at events and meetings run or hosted by us
- Your participation in rotas for service in the church
- Information contained in emails or other correspondence from you and records of telephone calls or meetings with you
- Your marital status, age, gender and information about your immediate family
- Details of money that you give to the church
- Information contained in checks provided by the Disclosure & Barring Service
- Information that you share with us for the purposes of pastoral care, encouragement, training and prayer
- Information relevant to your suitability for membership of and service in the church, employment by the church or service with other Christian organisations
- Medical information where necessary to ensure that the care and hospitality that we provide for you is appropriate to your needs
- Your receipt of goods or services that we provide, such as foodbank parcels or debt counselling
- Details of your visits to our website (including, but not limited to, traffic data, location data, weblogs and other communication data, whether this is required for our own purposes or otherwise) and the resources that you access.

How we get the personal information and why we have it

Most of the personal information we process is provided to us directly by you and we use it for one of the following reasons:

- To tell you about events that the church is running which we think may be of interest to you
- To provide pastoral care, support, teaching and challenge for you in accordance with the teaching of the Bible
- To enable us to maintain appropriate safeguarding arrangements for our children and young people and vulnerable adults
- To help you identify where you could serve in the life of the church
- To help us organise rotas and small groups and to communicate with you
- To help us receive donations and/or payments from you (and to make associated Gift Aid claims from HMRC)
- To help us ensure that you continue to meet the criteria for and obligations of membership (or where appropriate the qualifications for the office of elder)
- To provide you with practical support (e.g. foodbank parcels, debt counselling and speaking English)
- To provide you with a service (e.g. hire of our facilities).

We may share this information with others in the church including:

- To ask the members of the church to pray for you
- To enable the members of the church to provide pastoral care and support for you
- To inform the members of the church that you are applying to be a church member or that your membership has ended.

We may occasionally share your information with others outside the church including:

- When we are partnering with another organisation to provide you with goods or services (e.g. Trussell Trust re foodbank parcels and Christians Against Poverty re debt counselling)
- Where we are approached for a reference by another church or organisation
- With the contractor that hosts and maintains our website
- With the contractor that provides our text messaging service
- With HMRC in relation to Gift Aid claims.

Under the UKGDPR, the lawful bases we rely on for processing your information are:

- Your consent (which may be withdrawn at any time, by contacting us at the address given above)
- We have a contractual obligation
- We have a legitimate interest.

Hence, we will only collect and process your personal information if:

(i) you have given us your explicit consent,
(ii) we need to do so to fulfil a contract with you, or
(iii) we need to do so for the purposes of our legitimate interests outlined above.

For special category data falling within Article 9 of the UKGDPR, we consider that our collection and processing of it meets one or more of the following specified conditions:

- (a) Explicit consent
- (d) Not-for-profit bodies

When relying on condition (a), we will ensure that explicit consent is confirmed in a clear statement that is separate from any other consent being sought and specifies the nature of the special category data.

When relying on condition (d), we will:

- Only process special category data as part of our legitimate activities, i.e. those that fall within the purposes and powers set out in our constitution and are not unlawful or unethical in any way
- Limit such processing to the data of members, former members, or other individuals in regular contact with us in connection with our purposes
- Have appropriate safeguards in place
- Not disclose the data to a third party without the individual's explicit consent.

How we store your personal information

Your information is securely stored [enter location].

If you are a church member or regularly participate in our activities, we will keep your personal information for no longer than reasonably necessary, usually for the time that you are in church membership or participating in our activities. After this, we may continue to hold your contact details for as long as you agree, in order to keep you informed about the ministry of the church. We will then dispose of your information by physically destroying it or deleting it from our IT system.

If you are someone that benefits from our provision of goods or services, we will keep your [type of personal information] for [time period]. We will then dispose of it by physically destroying it or deleting it from our IT system.

Your data protection rights

Under data protection law, you have rights including:

- **Your right of access** - You have the right to ask us for copies of your personal information.
- **Your right to rectification** - You have the right to ask us to rectify personal information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete.
- **Your right to erasure** - You have the right to ask us to erase your personal information in certain circumstances.
- **Your right to restriction of processing** - You have the right to ask us to restrict the processing of your personal information in certain circumstances.
- **Your right to object to processing** - You have the the right to object to the processing of your personal information in certain circumstances.
- **Your right to data portability** - You have the right to ask that we transfer the personal information you gave us to another organisation, or to you, in certain circumstances.

You are not required to pay any charge for exercising your rights. If you make a request, we have one month to respond to you. Please contact us at the address above if you wish to make a request.

Our website may, from time to time, contain links to and from the websites of our partner networks, advertisers and affiliates. If you follow a link to any of these websites, please note that these websites have their own privacy policies and that we do not accept any responsibility or liability for these policies. Please check these policies before you submit any personal data to these websites.

How to complain

If you have any concerns about our use of your personal information, you can make a complaint to us at the address above.

You can also complain to the ICO if you are unhappy with how we have used your data, using the following contact details:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Helpline number: 0303 123 1113
ICO website: https://www.ico.org.uk

Appendix 13

Legitimate Interests Assessment (LIA)

Part 1: Purpose test

You need to assess whether there is a legitimate interest behind the processing.

• Why do you want to process the data? • What benefit do you expect to get from the processing? • Do any third parties benefit from the processing? • Are there any wider public benefits to the processing? • How important are the benefits that you have identified? • What would the impact be if you couldn't go ahead with the processing? • Are you complying with any specific data protection rules that apply to your processing (eg profiling requirements, or e-privacy legislation)? • Are you complying with other relevant laws? • Are you complying with industry guidelines or codes of practice? • Are there any other ethical issues with the processing?

Part 2: Necessity test

You need to assess whether the processing is necessary for the purpose you have identified.

• Will this processing actually help you achieve your purpose? • Is the processing proportionate to that purpose? • Can you achieve the same purpose without the processing? • Can you achieve the same purpose by processing less data, or by processing the data in another more obvious or less intrusive way?

Part 3: Balancing test

You need to consider the impact on individuals' interests and rights and freedoms and assess whether this overrides your legitimate interests.

First, use the DPIA screening checklist. If you hit any of the triggers on that checklist you need to conduct a DPIA instead to assess risks in more detail.

Nature of the personal data
• Is it special category data or criminal offence data? • Is it data which people are likely to consider particularly 'private'? • Are you processing children's data or data relating to other vulnerable people? • Is the data about people in their personal or professional capacity?

Reasonable expectations
● Do you have an existing relationship with the individual? ● What's the nature of the relationship and how have you used data in the past? ● Did you collect the data directly from the individual? What did you tell them at the time? ● If you obtained the data from a third party, what did they tell the individuals about reuse by third parties for other purposes and does this cover you? ● How long ago did you collect the data? Are there any changes in technology or context since then that would affect expectations? ● Is your intended purpose and method widely understood? ● Are you intending to do anything new or innovative? ● Do you have any evidence about expectations – eg from market research, focus groups or other forms of consultation? ● Are there any other factors in the particular circumstances that mean they would or would not expect the processing?

Likely impact	
● What are the possible impacts of the processing on people? ● Will individuals lose any control over the use of their personal data? ● What is the likelihood and severity of any potential impact? ● Are some people likely to object to the processing or find it intrusive? ● Would you be happy to explain the processing to individuals? ● Can you adopt any safeguards to minimise the impact?	
Can you offer individuals an opt-out?	Yes / No

Making the decision

This is where you use your answers to Parts 1, 2 and 3 to decide whether or not you can apply the legitimate interests basis.

Can you rely on legitimate interests for this processing?	Yes / No
Do you have any comments to justify your answer? (optional)	
LIA completed by	
Date	

What's next?

Keep a record of this LIA, and keep it under review.

Do a DPIA if necessary.

Include details of your purposes and lawful basis for processing in your privacy information, including an outline of your legitimate interests.

Appendix 14

Information Audit

DATA SUBJECTS	PERSONAL DATA HELD	DATA IS USED FOR	LAWFUL BASIS	WHERE HELD	HOW SECURED	WHO HAS ACCESS	RISKS?
e.g. Members							
e.g. Foodbank Clients							
e.g. CAP Clients							

Appendix 15

Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or relevant volunteer must immediately notify the Lead Elder or, in their absence, a Trustee
- The Lead Elder or a designated Trustee will investigate the report and determine whether a breach has occurred, i.e. whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The Lead Elder will immediately alert the Trustees to the situation, if a Trustee is not already investigating the matter
- The Lead Elder or Trustee will make all reasonable efforts to contain and minimise the impact of the breach and to assess the potential consequences
- The Lead Elder or Trustee will determine whether the breach must be reported to the ICO by assessing whether it is likely to negatively affect people's rights and freedoms and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned
- The Lead Elder or Trustee will document the decision (either way), in case it is subsequently challenged by the ICO or an individual affected by the breach
- Where the ICO must be notified, the Lead Elder or Trustee will do so by providing the specified information within the prescribed time limit
- The Lead Elder or Trustee will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the Lead Elder or Trustee will promptly inform all individuals whose personal data has been breached, providing them with written details
- The Lead Elder or Trustee will document every breach, recording the:
    - Facts and cause
    - Effects
    - Action taken to contain it and to prevent repetition (e.g. adopting more robust processes or providing further training)
- The Trustees will then meet as soon as reasonably possible to review what happened and to endorse the action being taken to prevent it from happening again

- The Trustees will also take action to mitigate the impact of different types of data breach, especially those involving sensitive information. For example:
    - If special category data is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
    - In any cases where the recall is unsuccessful, the sender will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way. The Lead Elder will ensure that a written response is received from all the individuals who received the data in error, confirming that they have complied with this request
    - If the sender is unavailable or cannot recall the email for any reason, the Lead Elder will take responsibility (seeking technical support as appropriate)
    - The Lead Elder will carry out an internet search to check that the information has not been made public; if it has, the publisher/website owner will be contacted and requested to delete the information and remove it from their website
    - Members of staff who receive personal data sent in error must alert the sender and the Lead Elder as soon as they become aware of the error.