GDPR: Local Group training manual

General Data Protection Regulation and the Privacy and Electronic Communications Regulations

The General Data Protection Regulation (GDPR) is a legal framework setting guidelines for the collection and processing of personal data relating to any individuals with in the European Union.
The Privacy and Electronic Regulations (PECR) sit alongside the Data Protection Act and GDPR. They give people specific rights in relations to electronic communications.

Personal data applies to both automated personal data and to manual filing systems.
GDPR and PECR require a much more transparent process for obtaining consent, requiring people to **positively opt in** to communications. Building on current data protection laws they also set out the rights of individuals and introduce tougher fines for non compliance.
The supervisory authority in the UK is the Information Commissioner's Office (ICO).

What is personal data?

Personal data refers to any information or attribute that can be used now or in the future to identify someone.
The official definition: 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

Put more simply: can you identify an individual from the information you hold on them?
If **yes** – then this falls under GDPR.
If **no** – then this falls outside of GDPR.

Personal data
This includes:

- a name and surname
- a home address
- an email address
- an identification card number
- age
- location data (for example the location data function on a mobile phone)
- an Internet Protocol (IP) address

Special sensitive data
Personal data deemed sensitive requires more protection because it poses a significant risk to a person's fundamental rights and freedoms. An organisation must be able to demonstrate the legal basis and the appropriate authority for doing so.
Special sensitive data relates to:

- data on children
- race or ethnic origin
- political opinions, including trade union membership
- religion or beliefs
- data concerning health or sexuality
- or criminal convictions or related security.

Principles of processing personal data

The Data Protection Act demands that personal data is processed in line with the following principles:

- **Lawfulness, fairness and transparency**
  - There must be a lawful basis for processing personal data. It must be processed fairly and individuals must understand when processing will occur.
- **Purpose limitation**
  - Personal data should only be collected for specified, explicit and legitimate purposes. It cannot be used or processed in a manner that is incompatible with such purposes.
- **Accuracy**
  - Personal data must be accurate and kept up to date.
- **Storage limitation**
  - Personal data should be kept for no longer than is necessary for the specified, explicit and legitimate purpose.
- **Integrity and confidentiality**
  - Personal data should be processed in a manner that ensures appropriate security of the data.
- **Accountability**
  - This is central to GDPR. Data controllers and processors are responsible for compliance with the principles and must be able to demonstrate this to data subjects and the regulator.

Changes introduced by GDPR and PECR

Data controllers and data processors

- GDPR introduces two new terms: data controllers and data processors
- Coeliac UK is the **Data Controller**
  - Coeliac UK determines the purposes and means of processing personal data and has specific obligations for ensuring data processors comply with the laws.
- Local groups are **Data Processors**
  - You are responsible for collecting, handling and maintaining personal data in line with current laws.

Local groups do not "own" data. Coeliac UK is responsible for **all** personal data whether provided to the central charity or collected by local group committee members. This includes personal data on non members, food industry professionals, venues and healthcare professionals. Anybody giving information to the local group, is giving their information to Coeliac UK; there is no way to differentiate between the two.

Local groups cannot own personal data separately from Coeliac UK.

A stronger lawful basis

GDPR outlines six legal basis for collecting personal data. Three are relevant to Coeliac UK and the charity's local groups:

1. Consent

- Consent means offering individuals real choice and control. Genuine consent should put individuals in charge, build customer trust and engagement, and enhance your reputation.
- GDPR and PECR set a high standard for consent
- Consent requires a positive opt-in. Don't use pre-ticked boxes or any other method of default consent.
- Individuals must know how to withdraw their consent.
- Clear and explicit consent is required for special sensitive data.

What consent means to you:

- Consent is required for any non members wishing to join your mailing list (including professionals and venue contacts etc).
- You **must use** the Coeliac UK mailing list sign up form.

2. Contract

- An organisation can hold someone's personal data in order to fulfil contractual obligations to them (eg providing manufacturers with a stall at your food fair or holding manufacturers details because they will be putting an advert in your newsletter) or because they have asked you to do something before entering into a contract (eg if you've contacted a venue requesting a quote to hire a room for an event).
- At Coeliac UK we have a contractual obligation to our members which incorporates Coeliac UK local groups as access to local groups is a part of the charity's membership offering
- At Coeliac UK we also have a contractual obligation with food industry professionals

What contract means to you:

- You have a responsibility to ensure members' data is kept up to date.
- The processing must be necessary and required for the task.
- Personal data must be deleted when it is no longer needed.
- Those relying on "contract" must be able to document and justify this basis.

3. Legitimate interest

- Legitimate interest applies when you use people's data in ways they would reasonably expect and which have minimal privacy impact or where there is a compelling justification for the processing.
- If you choose to rely on legitimate interests, you are taking on extra responsibility for considering and protecting people's rights and interests.
- Legitimate interest requires you to:
    - identify a legitimate interest
    - show that the processing is necessary to achieve it (if you can reasonably achieve the same result in another, less intrusive way, legitimate interests will not apply.)
    - balance your interest against the individual's interests, rights and freedoms. (If the individual would not reasonably expect the processing, or if it would cause unjustified harm, their interests are likely to override yours.)

What legitimate interest means to you:

When contacting members or processing personal data make sure you can:

- identify your interest
- show that processing necessary to achieve it
- demonstrate that your interest doesn't go against the individual's interests, rights and freedoms.

Greater say on the rights of individuals

Everyone has the right:

- to be informed about the collection and use of their personal data
- of access allowing them to see what is being held and how it's being used
- to rectification allowing inaccurate data or incomplete data to be updated within a month of the request being made
- to erasure – people can have their data permanently deleted
- to restrict processing – giving people greater say on how their data is being handled and used
- to data portability – allowing personal data to be moved, copied or transferred across IT systems
- to object to data being used for direct marketing or historical / scientific research or evidence
- to automated decision making and profiling.

Security

Security is key in ensuring the correct processing and handling of personal data. Data controllers and processors must ensure they have introduced appropriate measures to prevent:

- unauthorised or unlawful processing of personal data
- accidental loss of personal data
- destruction or damage to personal data.

What constitutes a breach?

There are eight key areas to be aware of:

- sharing data with an unauthorised 3rd party
- deliberate or accidental action (or inaction) by a controller or processor
- sending personal data to an incorrect recipient
- devices containing personal data (computer, laptop, mobile phone) being lost or stolen
- alteration of personal data without permissions
- holding data that is irrelevant to your role
- holding data that you have been asked to remove
- paper records containing personal data being lost, damaged or stolen.

A note on international transfer of data

GDPR and PECR imposes very strict conditions surrounding transferring data outside of the EU or to international organisations. **Local groups must not share data with unauthorised 3rd parties.**

Coeliac UK has taken the business decision to only use companies based in the EU and this extends to the local groups. As such Coeliac UK and local groups **cannot** use companies such as MailChimp or Survey Monkey as these countries store data in the USA. For more information on this please contact the Volunteering team at Coeliac UK.

What to do in case of a breach

You must notify Coeliac UK **immediately** if any data breach or complaint over the handling of data by an individual occurs. Phone or email the Volunteering team so that we can support you and get the issue properly recorded and resolved.

PECR and direct, personalised mailings

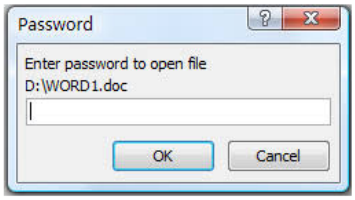
PECR introduces specific privacy rights in relation to electronic communications, including calls, emails, texts and faxes. PECR focuses on direct marketing, defined as "**the communication of any advertising or marketing material which is directed to particular individuals**."
This includes promotion of the aims, ideals, campaigning activity and fundraising asks by charities.

What PECR means to you:

You must be very clear with new contacts that by joining the local group mailing list they will receive information on the activities of the local group including support, awareness raising, fundraising and events.
We recommend against sending direct and/or fundraising or campaigning requests. Instead, put these asks within your general newsletters and forms. See our sign up form with donation request and welcome letter for examples of this.

What this means in practice: processing personal data in local groups

Saving, storing and sharing documents



It is your responsibility to ensure that any documents containing the personal data of committee members or local group contacts are kept as secure as possible.

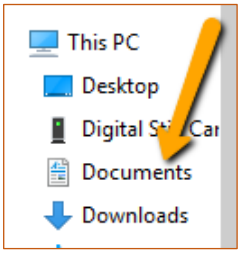
To this end, you must make sure:

- **personal data is limited to what is relevant and required**
- documents saved on computers or devices are **password protected**
- hard/paper copies of documents are **locked away**.

To note, any committee member can handle personal data provided they do so in compliance with GDPR and PECR.

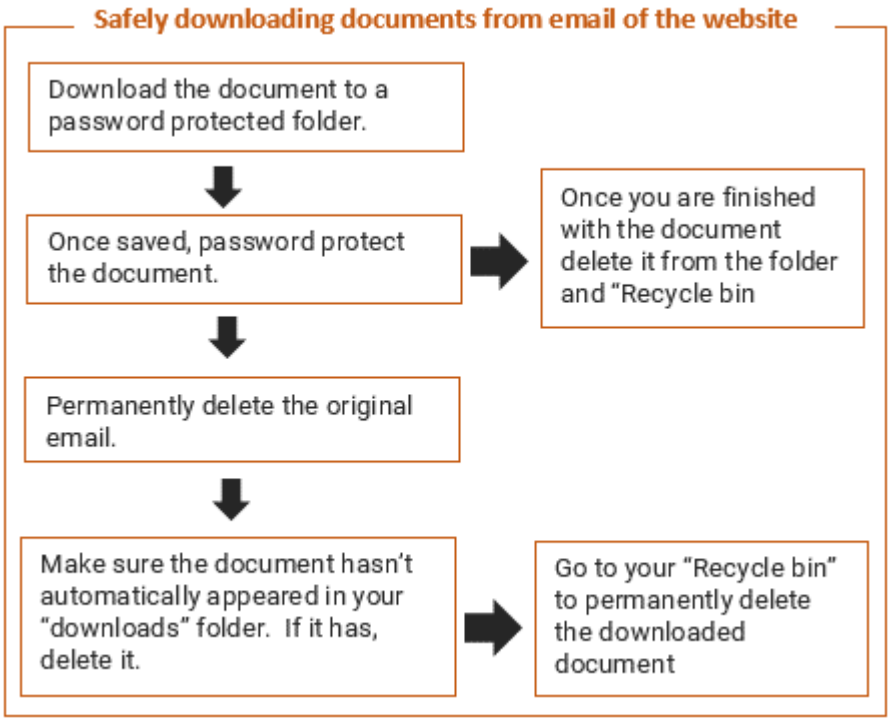
Creating and using documents containing personal data on your computer or device*

- When saving, make sure the document is **password protected**
- Save the document in a **password protected folder** in "Documents" or on a cloud platform and **not on your desktop**.
- Make sure you close the document when stepping away from your computer or device.
- **Permanently delete** the document when you no longer need it.
- Only access documents with personal data when on a secure internet connection e.g. at home or work. **Do not** access personal data when relying on 3G/4G.



*Please note as systems continue to be developed there will be less and less reason for any personal data to be secured on your personal computers and devices.

Downloading documents containing personal data from email or website



Sharing documents containing personal data over email

Email is **not** a safe way to send personal data. You must make sure:

- the email is sent from the localgroup@coeliac.org.uk email account
- that the document is **password protected**
- that you send the document and password in **separate emails**
- once sent you delete the email from your sent folder
- having deleted from your sent folder you then permanently delete from your "deleted" folder.

Sharing documents containing personal data through a cloud platform*

Cloud platforms such as Googledrive, Microsoft One Drive and iCloud, which you need a password to enter and where you can password protect your documents and folders are a good way to save documents in a location that can be accessed by multiple committee members.
If using a cloud platform make sure:

- you still password protect all documents and folders
- documents are permanently deleted when no longer needed
- the account is held in the local group name and not a personal account.

*As mentioned above as we develop our systems there will be less need to save any personal data on personal devices or cloud platforms.

Hard/paper copies of documents

- When in use at events, there should be a named committee member responsible for ensuring that paperwork containing personal data:
  - isn't left lying around
  - completed forms are put in a safe place.
- Any hard/paper copies of documents containing personal data (including letters, address labels and self addressed envelopes) must be saved in a secure location eg document safe, locked cupboard or locked filing cabinet.
- Once the document is no longer of use eg information has been transferred onto the computer, event has passed etc it must be destroyed.
- Destroying does not mean throwing away. The document must be burnt or shredded.

Local group emails

As we both work towards greater consistency and improved security, all local groups have been set up with a Coeliac UK webmail account, making your localgroup@coeliac.org.uk email account a full email through which you can send and receive local group emails.

Accessing your Coeliac UK Webmail account

Please see the associated guide for information on accessing and using your new email account.

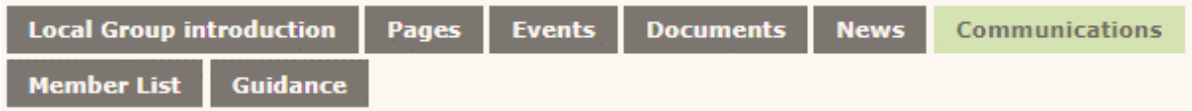
We would be grateful if you could move all emails and contacts over to your new account by **Saturday 1 September.**

The importance of BCC

Any emails sent to more than one contact, be they members, non members or food industry professionals, must be sent through the BBC field. Email addresses are "personal data" and revealing these to others is regarded as a breach of GDPR.

The only exception to this rule is when emailing amongst your local group committee members.

Sending bulk emails



The safest way to send emails to all contacts of the local group is through the Communications section of the Coeliac UK website.
Communications sent through the Coeliac UK website:

- are correctly branded
- contain a link to the Coeliac UK privacy policy
- allow people to opt out of emails, keeping your contact list accurate and up to date.

To note, changes are in the pipeline for a range of improvements to this area, which will be accompanied by updated guidance for all.

Providing reassurance in your communications

All communication sent by the local group, be that letters, emails, newsletters or event reminders, should include the following wording:

We care about your privacy, so we will keep your data secure. You can see our full Privacy Policy at https://www.coeliac.org.uk/privacy-policy/. You can update your personal details and preferences by logging into the Coeliac UK website, by contacting the local group or by phoning the Coeliac UK Helpline.

Local Group contact lists

What's not changing?

- Coeliac UK local groups will still be able to access personal data on members and supporters (non members, healthcare professionals) living in their area as well as local and national food industry professionals.
- Committee members will be able to use this information to send correspondence and better understand the demographic and geographic spread of contacts in their area.
- Local groups will be able to access the data through the Coeliac UK website.
- Access to local group contact lists will remain limited to **two** committee members per local group.
- Committee members will still be able to download a copy of local group contacts, however there are much stricter rules around doing so.

What is changing?

1. The name Membership lists will now become **Local group contact lists** including **all** members, supporters and contacts obtained either through Coeliac UK High Wycombe office or at the local level.

2. No separate local group and Coeliac UK lists Local groups will **not** be allowed to hold personal data on any individual separately from the charity. As outlined in the Coeliac UK Local Group Constitution, local groups are **not** a separate legal entity from Coeliac UK. By giving personal data to a local group, an individual is giving their personal data to Coeliac UK.

GDPR and PECR do not and cannot distinguish between the two.

Local groups will be able to obtain a full list of their member and non member contacts in their **local group contact list** on the website.

3. Tighter rules around downloading personal data
Committee members downloading contact lists onto their home devices:

- can only do so for a specified task
- must complete the task as quickly as possible (ideally no more than 48 hours)
- must password protect the document
- must download the data into a password protected folder
- must permanently delete the data once the task has finished.

4. Leavers. Under GDPR local groups will no longer be given the opportunity to contact leavers inviting them to remain on the local group mailing list. Instead, Coeliac UK will be providing members with a clearer say over what they want to hear about.
Leavers who have opted into "Community and events" communications will remain on the local group mailing list even after leaving Coeliac UK. (The only change you will see to their record is in relation to membership status).

Leavers who have not opted into "Community and events" will be removed from the local group mailing list. Local groups **do not** have permission to contact these people once they have left Coeliac UK.

3. The type of data you can hold on an individual

What you can hold:

- title
- first name and surname
- postal address
- email
- age
- phone number (either home phone or mobile – you shouldn't need both)
- Coeliac UK membership status
- other dietary requirements
    - to be gathered for specific events and not held against personal records
- data on children
    - information on children is categorised as **special sensitive data** and can only be collected with the explicit consent of their parent/carer. Information on children **must** be limited to the name and age of the child.

What you cannot hold:

The local group cannot hold any other information regarded as **special sensitive data:**

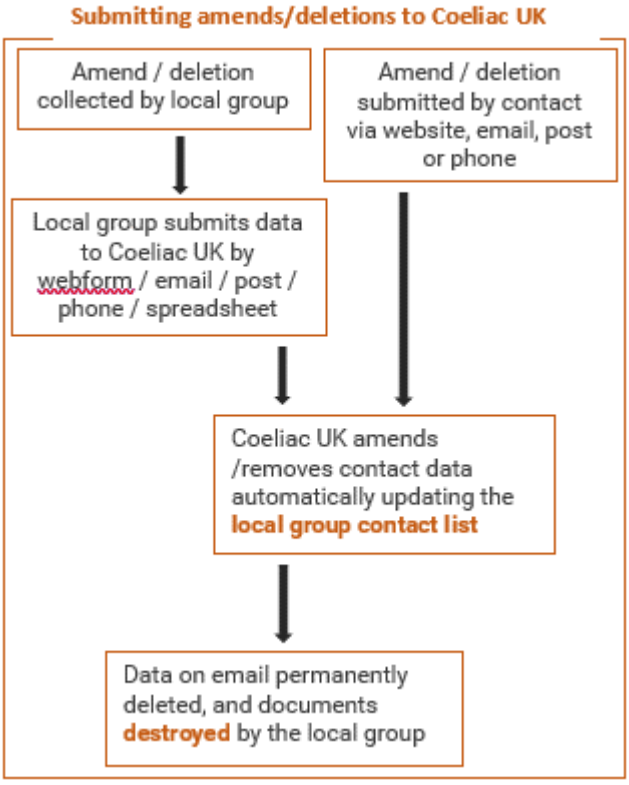
- medical information
    - We cannot guarantee that local groups can meet the strict requirements around the capturing and processing of medical information. As such you cannot ask people to declare on any forms or emails if they have coeliac disease or any other medical conditions (e.g. osteoporosis, diabetes…)
- ethnicity or race
- sexual orientation
- religious beliefs
- criminal history.

Keeping your local group contact list up to date

One of the core data protection principles is **accuracy**. If an individual gets in touch with the local group to update their details, be that a change of email address, postal address or change of name, Coeliac UK **must** be notified immediately (ideally within 72 hours) Similarly, if an individual asks to be removed from the local group mailing list, this must be processed immediately.

Contacts can update their details or remove themselves from the local group contact list at any time by:

- clicking the "opt out" option at the bottom of any emails sent by the local group through the Coeliac UK website
- logging into the Coeliac UK website and updating their communication preferences
- contacting the Coeliac UK Helpline or Volunteering team
- contacting the local group directly.



To help manage your contact lists we have also created template letters to confirm details with your contacts:

- Annual confirmation of details_with donation request
- Confirmation of details_non attendance_with donation request

(Paper copies of these must be printed **double sided** to be valid.)

We have also created spreadsheets for you to complete when returning details to the charity:

- New contact spreadsheet template highlighting all new contacts
- Local group contact amends and deletions template highlighting changes to existing contacts.

Committee members can notify the charity of a change in details by:

- completing the web form on the Coeliac UK website
- phoning the Coeliac UK Helpline / Volunteering team
- posting details; must be sent as "Signed for" delivery
- submitting details in a password protected spreadsheet. (Recommended when submitting more than five amends.) Please use the Local group contact amends and deletions template to help you with this.

Please do not send personal data in the body of an email.

Processing new members and new contacts

Adding new contacts to your local group

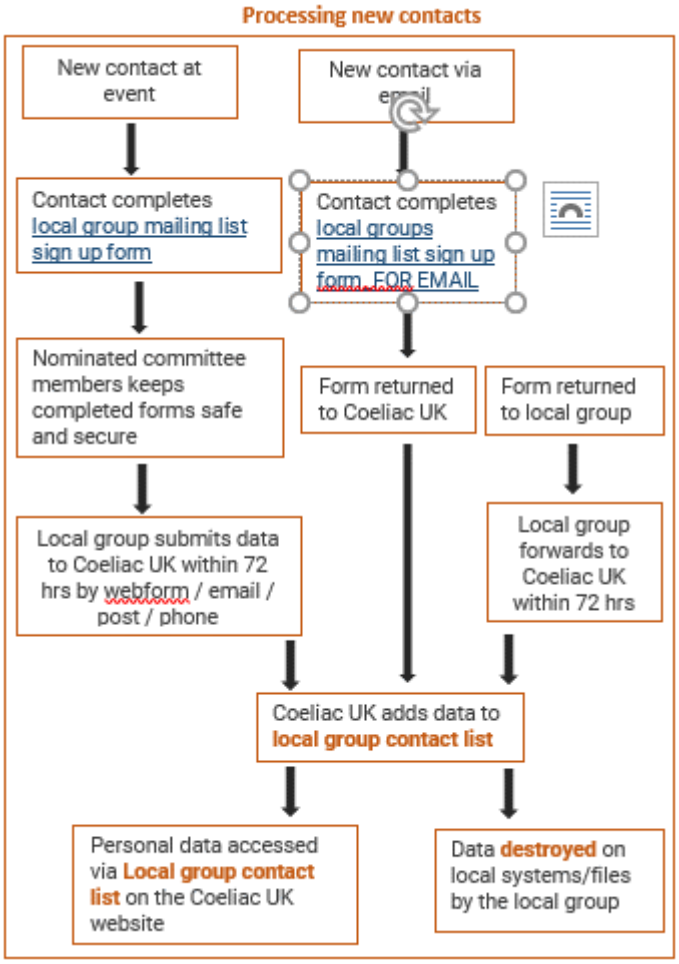
Forms for new contacts

Coeliac UK have developed a:

- local group mailing list sign up form
- local group mailing list sign up form_ WITH DONATION REQUEST
- local groups mailing list sign up form_FOR EMAIL (which can be amended and returned)

(Paper copies of these must be printed **double sided** to be valid)

These forms are GDPR and PECR compliant and are the **only forms** local groups can use to gather **new** contact information. The Volunteering team will be in contact to ensure they are personalised correctly for your committee.



Processing new contact data at events

There should be a named committee member at each event, responsible for ensuring paper forms are safe from loss, damage or misuse. Completed local group mailing list sign up forms **should not be** left out for passers by to see, instead they should be put out of sight. Following the event they should be submitted to Coeliac UK as soon as possible (ideally within 72 hours). For information on how to do this please see above, **Keeping your local group contact list up to date** and remember to use our New contact spreadsheet template.

Processing personal data over email

Non members getting in touch with a local group for the first time through email, should be sent the local groups mailing list sign up form_FOR EMAIL. This form has been created so people can update their details directly onto the form and return.
As per the instructions on the form, completed forms should be sent directly to Coeliac UK.
Any forms accidentally returned to the local group should be forwarded to Coeliac UK immediately. Coeliac UK will then confirm the safe arrival of the form with you. Once this confirmation has been received please delete the original email from your "sent" folder and "deleted" items immediately.

New member and new contact welcome letters

Coeliac UK can send automated welcome letters to new members and contacts on behalf of your local group. For more information on this, please contact volunteering@coeliac.org.uk

If you wish to send your own new local group contact mailings, then you are welcome to use our Local group welcome letter_Coeliac UK member and our Local group welcome letter_new member contact as a guide. Please remember that all mailings must include our **privacy statement.**

Running events

Invitation to events

You can promote your events to anybody on your local group contact list as well as promoting publically. You can promote as part of your newsletter or by direct mailings (email or post).

With all mailings you must give people the opportunity to opt out of your mailing list, so **remember to include the privacy statement**.

Booking information needs to be saved in a **password protected Word or Excel document**. As always, make sure you **only** capture essential information (which if your mailing list is up to date, should just be name, meal choices and payment confirmation – if applicable). You don't need people's postal addresses and date of births to confirm a dinner booking. We've created a few templates for you:

- Event booking template with menu choice and payment
- Event booking form no menu choice and payment

For children's events see below.

Be very clear about what response you need and when you need it by. Best practice holds that people should only reply if they are planning on attending. **Those who can't attend, shouldn't have to reply.**

Medical information or dietary preferences

Local groups do not have permission to capture medical information. As per our template letter, please make sure that you **do not** ask if people are diabetic / lactose intolerant etc but instead ask an open question as to whether they have other dietary requirements.
Under GDPR individuals volunteering dietary preferences for a specific event are **not** giving permission for local groups to hold this information against their record. This information should **only** be gathered if required and should only be kept for the specific event.

Whilst we appreciate that postal recipients or those paying by cheque will need a committee member's address to send their information to, please make sure this information is **removed** before forms are uploaded onto the Coeliac UK website or social media accounts.

Handling booking responses

As above, any committee member can handle personal data provided they do so in compliance with GDPR and PECR. There should be a named committee member, with overall responsibility for receiving and handling all returns, both by email and post. Use the Event booking form template to help you manage returns.

Email replies
Returned booking forms should be sent to the localgroup@coeliac.org.uk email account and not to a personal email account. Information should be transferred to a password protected file and the original form permanently deleted.

Postal replies
Postal replies should be uploaded into **a password protected file** and then the original form permanently deleted or destroyed.

Sending information to the venue
We appreciate that venues often need menu choices and table plans in advance. If sending this information over to the venue, strip away as much personal data as possible. Please use the Venue confirmation template to guide you.

Invitation to children's events
Please remember that you **cannot** write directly to the child. All correspondence **must** be directed to the parent/carer.
You should only ask for their child's age if that information is essential for your event. Do not ask for date of birth, instead ask for age which is safer from a data protection perspective.
Please use our template to help you: Local events booking form_childrens event

After the event
After the event, please make sure you **delete** all information that is no longer needed. Paper documents relating to the event should be destroyed, emails and documents saved on your computer permanently deleted.

Keeping a log of booking attendance
We have created a spreadsheet for you to keep track of who is attending your events: Annual event attendance record. This information should be limited to the name of your contact and the type of event. No further information should be required.

Wherever possible don't use personal data, if personal data can't be avoided keep it as safe as possible – password protected or locked away.

Registration form at events

As part of health and safety or fire regulations, local groups often ask people to sign in to events. The registration list should not be confused with collecting details to add people to the local group mailing list.
Please use the meeting registration template provided, for registration at general meetings and AGMs, which you will see keeps personal data to an absolute minimum asking only for surname, minimal contact information and if a member or not. The form must be destroyed (shredded or burnt) after the meeting.

Photography consent at events

You must secure permission from all attendees before taking any photos at events. This is crucial if the photos are going to be uploaded onto social media or promoted on Coeliac UK local group and Coeliac UK publications or webpages.

- Photography consent form for adults
- Photography consent form for children.

Where to go for help: If you have any questions or queries please contact the Volunteering Team at volunteering@coeliac.org.uk or phone 01494 796 117 / 01494 796 118.