Landward Research

DATA PROTECTION POLICY

Data Protection Policy
Reviewed February 2022
Next Review February 2025

LANDWARD RESEARCH
UNLOCKING CULTURAL VALUE

Table of Contents

1 Introduction

Landward Research is a trading name of Landward Research Ltd (a company registered in England and Wales with company number 03749035 whose registered office is at 120 Bradley Street, Sheffield S10 1PB, United Kingdom) and its group companies, Landward Research Teoranta with a registered office in Ireland (IE) and Landward LLC with a registered office in New Mexico (USA), (hereafter referred to as "Landward Research", "we" or "us") is committed to protecting and respecting your privacy and we take all reasonable precautions to safeguard personal information.

Landward Research provide Labour Market Intelligence, Project Management and other consultancy services to its clients. The personal data that Landward Research processes to provide these services relates to its clients and other individuals as necessary, including staff and suppliers' staff.

This policy and any other documents we refer to in this policy, including the Market Research Society Code of Conduct, set out how we will use your personal information and who it will be shared with.

This policy sets out Landward Research's commitment to ensuring that any personal data, including special category personal data, which Landward Research processes, is carried out in compliance with data protection law.

Landward Research ensures that good data protection practice is imbedded in the culture of our staff and our organisation. Every member of staff has a responsibility to adhere to the Data Protection Principles outlined in the GDPR, and to this Data Protection Policy

Under the General Data Protection Regulation (GDPR) and Data Protection Act (DPA) 2018, Landward Research registered with the Information Commissioner's Office (registration number: Z2502970) as a Data Controller and must comply with data protection legislation.

2 Scope

Within the policy, 'Data' are defined as information collected in any nature or format.

This policy applies to all personal data processed by Landward Research and is part of Landward Research's approach to compliance with data protection law. All Landward Research staff are expected to comply with this policy and failure to comply may lead to disciplinary action for misconduct, including dismissal.

This procedure applies equally and fully to Landward Research Ltd and to all subsidiary companies of Landward Research Ltd (on 14th February 2022: Landward Research Teoranta, Landward Limited Liability Company and Landward Limited).

3 Data Protection Principles

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).

Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- Used fairly, lawfully and transparently
- Used for specified, explicit purposes
- Used in a way that is adequate, relevant and limited to only what is necessary
- Accurate and, where necessary, kept up to date and that reasonable steps will be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
- Handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

We are committed to upholding the Data Protection Principles. All personal data under our control must be processed in accordance with these principles.

Landward Research will facilitate any request from a data subject who wishes to exercise their rights under data protection law as appropriate, always

communicating in a concise, transparent, intelligible and easily accessible form and without undue delay.

3.1 Special Category Personal Data

There is stronger legal protection for more sensitive information, such as:

- Race
- Ethnic background
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- The processing of genetic data, biometric data for the purpose of uniquely identifying a natural person
- Health
- Sex life or orientation

There are separate safeguards for personal data relating to criminal convictions and offences.

Landward Research processes special category data of clients and third parties as is necessary to provide services.

Landward Research processes special category data of employees as is necessary to comply with employment and social security law. This policy sets out the safeguards we believe are appropriate to ensure that we comply with the data protection principles set out above. Landward Research has a data retention policy which sets out how long special category data will be held onto.

4 Data Subject Rights

Landward Research has processes in place to ensure that it can facilitate any request made by an individual to exercise their rights under data protection law. All staff have received training and are aware of the rights of data subjects. Staff can identify such a request and know who to send it to.

All requests will be considered without undue delay and within one month of receipt as far as possible.

Subject access: the right to request information about how personal data are being processed, including whether personal data are being processed and the right to be allowed access to that data and to be provided with a copy of that data along with the right to obtain the following information:

- Purpose of the processing
- Categories of personal data
- Recipients to whom data has been disclosed or which will be disclosed
- Retention period
- Right to lodge a complaint with the Information Commissioner's Office
- Source of the information if not collected direct from the subject, and
- Existence of any automated decision making

Rectification: the right to allow a data subject to rectify inaccurate personal data concerning them.

Erasure: the right to have data erased and to have confirmation of erasure, but only where:

- The data are no longer necessary in relation to the purpose for which it was collected, or
- Where consent is withdrawn, or
- Where there is no legal basis for the processing, or
- There is a legal obligation to delete data

Restriction of processing: the right to ask for certain processing to be restricted in the following circumstances:

- If the accuracy of the personal data are being contested, or
- If our processing is unlawful but the data subject does not want it erased, or
- If the data are no longer needed for the purpose of the processing but it is required by the data subject for the establishment, exercise or defence of legal claims, or
- If the data subject has objected to the processing, pending verification of that objection

Data portability: the right to receive a copy of personal data which has been provided by the data subject and which is processed by automated means in a format which will allow the individual to transfer the data to another data controller. This would only apply if Landward Research was processing the data using consent or on the basis of a contract.

Object to processing: the right to object to the processing of personal data relying on the legitimate interests processing condition unless Landward Research can demonstrate compelling legitimate grounds for the processing which override the interests of the data subject or for the establishment, exercise or defence of legal claims.

You should direct any request for your information to us at enquiries@landward.eu. Please note that a fee of ten pounds (£10.00) may be payable to meet our costs in providing you with details of the information we hold about you.

You have the right to require us to remove all information we have about you. Direct any request for us to remove your data to us at enquiries@landward.eu.

If you have a complaint about how we have used your information, you have the right to complain to the Information Commissioner's Office.

5 Lawful Processing

All processing of personal data must meet one of the six lawful bases defined in Article 6(2) of the GDPR:

- Where we have the consent of the data subject
- Where it is in our legitimate interests, and this is not overridden by the rights and freedoms of the data subject.
- Where necessary to meet a legal obligation.
- Where necessary to fulfil a contract, or pre-contractual obligations.
- Where we are protecting someone's vital interests.
- Where we are fulfilling a public task, or acting under official authority.

Where processing is based on consent, the data subject has the option to easily withdraw their consent.

Where electronic direct marketing communications are being sent, the recipient has the option to opt-out in each communication sent, and this choice will be recognised and adhered to by us.

6 Responsibilities

6.1 Landward Research Company Responsibilities

As the Data Controller, Landward Research is responsible for establishing policies and procedures in order to comply with data protection law.

6.2 Staff Responsibilities

Staff members who process personal data about any individual must comply with the requirements of this policy. Staff members must ensure that:

- All personal data are kept securely;
- No personal data are disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party;
- Personal data are kept in accordance with landward research's retention schedule;
- Any queries regarding data protection, including subject access requests and complaints, are promptly directed to the CEO;
- Any data protection breaches are swiftly brought to the attention of the CEO and that they support the CEO in resolving breaches;
- Where there is uncertainty around a data protection matter advice is sought from the CEO.

Staff who are unsure about who are the authorised third parties to whom they can legitimately disclose personal data should seek advice from the CEO.

6.3 Third-Party Data Processors

Where external companies are used to process personal data on behalf of Landward Research responsibility for the security and appropriate use of that data remains with Landward Research.

Where a third-party data processor is used:

- A data processor must be chosen which provides sufficient guarantees about its security measures to protect the processing of personal data;
- Reasonable steps must be taken that such security measures are in place;

- A written contract establishing what personal data will be processed and for what purpose must be set out;
- A data processing agreement must be signed by both parties.

7 What Information We Collect

We may collect and process the following data about you ("your information"): Contact details including your name, address, email address and telephone number;

- Information you provide when participating in specific Landward Research polls, panels or other forms of Landward Research work. Participation in such panels, activities and polls is completely voluntary and some such activities may involve you providing sensitive personal data including information about your age, gender, ethnicity, disability status, religion or belief, sexual orientation and country of origin;
- Information you provide when you complete your profile on the website or access your social media content via the website; and
- Information you provide relating to your opinions, attitudes, experiences and use of certain products or services;
- Information you provide relating to your opinions, attitudes, experiences and use of certain products or services
- Your email address and subscription preferences when you sign up to our newsletter
- How you use our emails - for example whether you open them, and which links you click on
- Your internet protocol (IP) address, browser type, internet service provider (ISP), referring/exit pages, operating system, date/time stamp, and clickstream data

- Information on how you use the site, using cookies[1], web beacons[2] and page tagging techniques

We may collect your information via the following methods:

- Information that you submit online via our site or by participating in Landward Research activities or polls that may be delivered through third-party online survey partners;
- Any correspondence you send to us;
- Details of your visits to our site (and third-party websites which link to our site) and the resources that you access (which may include, amongst other things: traffic data and communication data);
- Information you post on our site;
- Details of transactions you carry out or orders you place through our site; and
- Information you provide to us via social media or through your social media feed
- Information given by employee of ours if they give your contact details as an emergency contact or a referee

We are aware that your information may be confidential, and we will protect the confidentiality of your information in accordance with our normal procedures and legal requirements. We will not use it for any purposes other than those set out in this policy.

We will process your information in accordance with the Data Protection Act 2018 and the Market Research Society Code of Conduct.

---

[1] Our site may use "cookies" to enhance user experience. User's web browser places cookies on their system for record-keeping purposes and sometimes to track information about them. Users may choose to set their web browser to refuse cookies, or to alert you when cookies are being sent. If they do so, note that some parts of the Site may not function properly.

[2] Our site may use web beacons to collect non-personal information about the use of our services. The information collected by web beacons allows us to monitor how many people are using our services, how many people open our e-mails, and determine for what purposes these actions are being taken. Our web beacons are not used to track activity outside of our services. We do not link non-personal information from web beacons to personally identifiable information without permission and do not use web beacons to collect or store personally identifiable Information.

8 How We Use Personal Data

We use your information in the following ways:

- To provide services to our clients (please also see section below headed "Who We Share Personal Data With");
- To analyse the data for research purposes and to incorporate it into our databases for general research and analysis purposes;
- To ensure that our site's content is presented as effectively as possible for you;
- To deal with any complaints, queries or technical problems you experience;
- For our internal purposes, such as quality control, site performance, system administration and to evaluate use of our site and its efficiency, so that we can provide you with enhanced services and a better experience;
- To notify you about changes to our services or changes which may affect your participation in Landward Research activities;
- To provide you with information, research products or services that you request from us, or which we feel may interest you;
- To provide you with Landward Research project results;
- To create reports to assist with future marketing; and
- To send you invitations to take part in our surveys, polls or activities and to update you on issues relating to those activities.

We may monitor your use of our site and record your email address and/or IP address, operating system and browser type, for system administration. This is statistical information about our users' browsing actions and patterns and does not identify any individual.

We only keep your information for as long as is necessary.

Your information may be accessed and processed by our staff, service providers, affiliates or agents located in any of our offices around the world.

Please do not send us your information if you do not agree to it being transferred outside the EEA in this way. By providing your information to us you agree and consent to us transferring to, and storing your information in any of our offices around the world. If you do not agree to this then you should unsubscribe from the Landward Research panel.

9 Security Precautions In Place To Protect The Loss, Misuse, Or Alteration Of Personal Data

Landward Research takes all reasonable steps to protect the privacy of visitors to our website, but we cannot promise that the current limitations of the software that runs our website will address every browser setting or honour every personal browser preference. As the capabilities of our software improves, we will take all reasonable steps to honour such requests in the future. Please return to this privacy policy for further updates on this topic.

When you give us personal information, we take steps to ensure that it's treated securely. Any sensitive information (such as credit or debit card details) is encrypted and protected with the following software 128 Bit encryption on SSL. When you are on a secure page, a lock icon will appear on the bottom of web browsers such as Microsoft Internet Explorer.

Non-sensitive details (your email address etc.) are transmitted normally over the internet, and this can never be guaranteed to be 100% secure. As a result, while we strive to protect your personal information, we cannot guarantee the security of any information you transmit to us, and you do so at your own risk. Once we receive your information, we make our best effort to ensure its security on our systems. Where we have given (or where you have chosen) a password which enables you to access certain parts of our websites, you are responsible for keeping this password confidential. We ask you not to share your password with anyone.

10 Who We Share Personal Data With?

We may share your information with any companies in our group and other branches of Landward Research for internal reporting purposes.

We may share your information with other organisations:

- Who provide services to us so that they can provide the services we request. This might include it service providers who support our ICT systems, for example;
- Who we provide services to so that they can benefit from the services we provide. Whilst we will, where possible, take steps to ensure that you cannot be identified from that information, as we cannot ever fully understand what information our clients may already hold about you, it may be that they can link

the anonymous information that we provide, to other information which then enables them to identify you. By way of example:

- We may exchange what we consider to be anonymous or pseudonymised information about our panellists with third parties who will use it for analysis purposes, to enhance their own databases, to model audiences and track the efficiency of campaigns, and to gain an insight into behaviours so that they can develop strategies which add value to their, or their clients' businesses. For this purpose, we may also collect anonymised information from third parties which we can use to identify you. As our clients and, in turn their clients, will have their own databases and other sources of information, it may be that they could link the anonymous information we provide with information they already have and therefore identify you; or
- We may provide limited personal details to trusted third party data processors for the purposes of combining our data with other third-party data sources. The final combined data set will be anonymised and non-attributable.

- If we sell or buy any business or assets, (as we may share your data with the prospective seller or buyer);
- If we or substantially all of our company assets are acquired by another party, in which case your information will be one of the transferred assets; or
- If we have to share your information to comply with legal or regulatory requirements (or we reasonably believe that we need to disclose your information for such purposes), or if we have to enforce or apply any other terms and conditions or agreements or to protect our rights, property or our customers etc.

Other than as listed above, we will not rent, sell or otherwise disclose your information without your consent.
Please bear in mind that whenever you voluntarily disclose personal data online – for example on message boards, on a blog or chat area – that information will be viewed by others.

11 Asking For Consent

11.1 In Our Panels Or Surveys

- We check that consent is the most appropriate lawful basis for processing

- We make the request for consent prominent and separate from our terms and conditions
- We ask you 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 individual ('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 you that you can withdraw your consent
- We ensure that you 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.

11.2 Recording Consent

- We keep a record of when and how we got consent from you
- We keep a record of exactly what you were told at the time

11.3 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 consider using privacy dashboards or other preference-management tools as a matter of good practice
- We make it easy for you to withdraw your 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 you if you wish to withdraw consent.

12 Landward Research Marketing

You have a choice about whether or not you wish to receive information from us. If you do not want to receive direct marketing communications from us about our

work, products and services, then you can select your choices by ticking the relevant boxes situated on the form on which we collect your information.

We will not contact you for marketing purposes by email, phone or text message unless you have given your prior consent. We will not contact you for marketing purposes by post if you have indicated that you do not wish to be contacted. You can change your marketing preferences at any time by contacting us by email to enquiries@landward.eu or by writing to Landward Research Ltd, 120 Bradley Street, Sheffield S10 1PB, UK.

13 Communicating With You

By participating in a Landward Research poll or survey, you agree to allow us to communicate with you via email or SMS in relation to your participation in the Landward Research poll or survey(s) and opportunities to participate in Landward Research activities. These include but are not limited to communications relating to:

- Landward Research polls or surveys
- other forms of Landward Research work
- Landward Research project results
- Landward Research newsletters

14 Data Breaches

Any data breaches or suspected data breaches should be immediately managed and reporting in accordance with the Data Breach Incident Response and Reporting Procedure (ANNEX I).

Third parties will report any data breaches or suspected data breaches to Landward Research on 07803895033 or, if there is no answer, emailing Kenneth.aitchison@landward.eu. A third party reporting a data breach or suspected data breach must also inform their Landward Research point of contact by phone or email.

Breaches will be managed in accordance with the Data Breach Incident Response and Reporting, which includes, where necessary, notifying the ICO within 72 hours of a breach being known.

15 Breaches of Policy

Failure to follow any of the applicable Landward Research policies by staff members may result in disciplinary action. A data breach by a third party may result in a termination of contract and/or compensation claim.

16 Other Related Documentation

Where necessary, this policy should be read in conjunction with other Landward Research Policies, such as:

- Performance Management Procedure
- Code of Conduct
- Equity, Diversity, and Inclusion Policy

17 Review

Landward Research will review this policy on an ongoing basis and carry out a formal review not less than every 3 years. Such review shall take into account the operation of the Policy since the last formal review, any legal or regulatory developments, an assessment of current best practice and any other relevant information.

18 ANNEX I: Data Breach Incident Response And Reporting Procedure

The Information Classification Table (ANNEX II) defines 'restricted information' and 'highly restricted information'.

18.1 What Is A Data Breach?

A data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, data. Breaches may be the result of accidental or deliberate causes. A data breach is not limited to personal data. Examples include:

- Sending an email containing restricted information or highly restricted information to the wrong recipient (i.e. someone who should not have access to that data), where the information is not password protected in an attachment or the password has also been sent to the wrong person
- Loss or theft of phone, laptop, tablet, USB or other external hard drive containing restricted or highly restricted data
- Retaining work-related personal data on a staff member's own device when the personal data are about someone else
- Making personal data / confidential business information publicly available on a website where consent has not been given (if needed)
- Alteration of personal data without appropriate authorisation
- Telling someone a password which allows unauthorised access to restricted or highly restricted information
- Restricted information or highly restricted information which is needed and has been lost, destroyed or corrupted when it cannot be retrieved / another copy is not available
- Restricted information or highly restricted information that has been inappropriately disclosed or accessed whether electronically or in hard copy.

The disclosure of truly anonymised information about individuals may not be a breach of personal data but could be a breach of business confidentiality. If you are unsure whether a disclosure of this type constitutes a reportable breach, you need to liaise with line manager straight away. The recipient of the data should be requested to securely dispose of and confirm disposal of the information.

18.2 Data Breach Incident Response And Reporting

If possible, immediately speak to your line manager to decide how to limit the potential breach. Even if they are not available you still need to decide how to limit the potential breach.

If data has been shared with someone who should not have access to the data, you need to immediately phone the recipient requesting them to permanently delete the email including any attachments and to respond to you confirming they have done so. If it is not possible to contact them by phone, you need to email them requesting them to do both of these things. Phoning is preferable as it may speed up the response and mean they are less likely to open the email at all. You need to do this even if the information is pseudonymised or password protected. If the recipient has received a password protected attachment but not the password, them deleting the email is the end of the situation.

If you have deleted data which should not have been deleted, or the data has corrupted (and therefore is not available) consider where else this data may be stored or backed up. Arrange for the data to be returned. If it is not possible to retrieve the data you need to ask advice from your line manager.

If you discover that data are out of date (and are not being stored for historical purposes when a 'snapshot in time' might be appropriate) you need to make reasonable effort to update the information. This includes liaising with other areas of Landward Research who may also be storing the data to find out whether they have updated data or to inform them of the update. If the data cannot be updated you need to seek advice from your line manager about whether this data should continue to be securely stored, or securely destroyed.

If the data breach or suspected data breach is of another kind, contact the CEO for advice.

If you cause, receive or notice a data breach or suspected data breach you should report it as a matter of urgency.

Data breaches and suspected data breaches should be reported as soon as possible, directly after any action you have taken to limit the breach.

You must report any information security incident that you suspect has affected the confidentiality (security), integrity (accuracy) or availability of data.

18.3 How To Report A Data Breach Or Suspected Data Breach

Telephone the CEO (07803 895033) or if there is no answer then email Kenneth.aitchison@landward.eu.

When making a report, **do not include** 'restricted information' or 'highly restricted information' relating to the breach. Check for attachments and remove them. If you do include the breached data you are causing another data breach.

Include as much of the following information as possible (it is important you report the breach or suspected breach straight away even if you do not have all the information):

- The date and time of the data breach
- How the data breach occurred
- What type of 'restricted information' or 'highly restricted information' is involved
- The number of data subjects affected
- The number of data records affected (e.g. a breach involving the name, date of birth and address of 5 people would be 15 data records)
- Who has been given access to the information who should not have access
- Whether you know that the information has been accessed
- What remedial action you have taken
- Any other information you think is relevant.

18.4 Why Report Suspected Data Breaches And Data Breaches

Sometimes it is hard to know exactly what has happened. Therefore even if you only suspect a data breach has occurred it is best to report it so that any negative impact can be prevented. If it turns out that there was no data breach after all, nothing has been lost in reporting it.

The data subject / organisation remains increasingly vulnerable, the longer a data breach is uncontained and unreported. This may lead to further sharing of the restricted or highly restricted information.

The General Data Protection Regulation (GDPR) places a duty on organisations to report certain types of personal data breach to the Information Commissioner's Office within 72 hours of becoming aware of the breach. Suspecting or knowing that a breach has occurred and delaying reporting reduces the time available for the CEO to understand and assist with a response and still meet legal compliance.

Where the breach does not affect personal data, time is still critical and may have contractual or legal implications.

Understanding the cause of data breaches allows us to develop and implement systems and processes that are more robust and prevent future breaches / reduce the risks associated with breaches.

18.5 After Reporting A Data Breach Or Suspected Data Breach

The CEO will respond to you and support you in managing the situation. Depending on the severity of the personal data breach, they may need to notify the Information Commissioner's Office, for which there is a 72-hour deadline from the time the first person in the organisation knows of the personal data breach.

Therefore if you have reported a personal data breach or suspected personal data breach it is vital that you check your email for a response from the CEO, even if this means checking over the weekend. The CEO may require more information from you or ask for your assistance in completing the data breach reporting form.

The CEO, together with the appropriate staff (*e.g.* Director of Analysis, Research and Technology, Operations and Strategy Manager) will make an initial assessment to determine the next steps. The severity of the incident will determine whether or not it needs to be reported to the Information Commissioner's Office.

The reporting of the data breach will help to improve best practice across Landward Research.

19 ANNEX II: Landward Research Information Classification Table And Handling Procedures

The Information Classification Table starts on page 24.

19.1 Headlines About Access And Security

Computer Access: Highly restricted information must have access controls (*e.g.* should be password protected / pseudonymised in an email, should need a log on to access in a database, should be in a OneDrive folder only accessible by those who need it etc).

Electronic Portable Storage: As per the Information Security Policy clause [xxx] Removable Storage media containing 'restricted information' or 'highly restricted information' must be encrypted with inbuilt encryption or software such as 'Bitlocker' or password protected before being removed off-site. Bitlocker is a free Windows facility, instructions for which are on the Microsoft Support page Device encryption in Windows.

Printing: Caution should be taken when printing Restricted or Highly Restricted information. Printing should only take place when necessary *i.e.* for a purpose when accessing the information electronically is either not possible or not practical. If you print Restricted or Highly Restricted information, you need to know the location of the physical document. It needs to be disposed of in a cross-shredder.

Paper Access: Paper copies of restricted information should be out of sight. Paper copies of highly restricted information should be in locked storage when not being used.

Hard-copy storage: For Restricted or Highly Restricted information, if an electronic copy is stored, there should only also be a hard-copy if absolutely necessary and this copy should be in a locked cabinet or room with access limited to those are authorised to see the document.

Sharing: Caution should be taken when sharing Restricted or Highly Restricted information. Consider whether the recipient should have access to the information and, if so, provide clear instructions as to whether or not they have authority to share it, and with whom and how they should store and dispose of it.

Disposal: All hard copies of Restricted and Highly Restricted information must be cross-shredded when no longer required. All electronic copies must be deleted. Please note if your desktop recycle bin is set to retain deleted files, this bin automatically permanently deletes its contents once a month.

19.2 Definitions Of The Classifications And How To Email

Information Classification	How to email this type of information
Ordinary information is information which is unlikely to identify an individual, is in the public domain or would be unlikely to have a negative impact on the rights and interests of individuals or the interests of Landward Research	**Ordinary information** can be in the body of an email containing the data subject's name. No particular controls, other than common sense, apply to 'ordinary information'. However 'ordinary information' should be treated as restricted or highly restricted when combined with information from either of those categories.
Restricted information is information which if disclosed to unauthorised recipients could have a negative impact on the rights / interests of individuals or the interests of Landward Research and would likely be a data breach under data protection laws or a breach of commercial confidentiality. 'Restricted information' must be classified as 'highly restricted' when it covers 30 or more individuals and is being emailed or transferred by external hard drive / USB *etc.*	When emailing restricted information, do not put the data subject's name in the email subject line. It is up to your professional judgement of the context of the personal data in the email whether you should use the methods described for 'highly restricted information'. Please refer to the footnotes of the Information Classification Table and then ask your line manager if you are unsure.
Highly restricted information is information which if disclosed to unauthorised recipients would be likely to result in serious damage to the rights and interests of	1. If the recipient can access this directly from the Landward Research Ltd OneDrive or SharePoint, then they must access it this way and it must not be emailed.

individuals or of the interests of Landward Research and would very likely be a data breach under the GDPR or a breach of commercial confidentiality.	2. If the content is personal data and you use the data subject's name in the email, this content must be in a password protected attachment (with the password sent in a separate email). 3. If the content is personal data do not use the data subject's name in subject line. 4. Where the content relates to non-personal data (e.g. it is commercially sensitive) the information must be attached as a password protected document.

N.B. A set of 30 or more records of 'restricted information' should be treated as 'highly restricted information'.

19.3 Information Classification Table

Ordinary Information (non-exhaustive examples)	**Restricted Information** (non-exhaustive examples)	**Highly Restricted Information** (non-exhaustive examples)
Anonymised data[3]	Name, Home address and / or phone number[4]	Financial Information regarding individuals
Data agreed by data subjects to be put into the public domain	Corporate contact details where the personal information is not available publicly and identifies an individual	Information identified in Equality Act 2010 as

[3] For these purposes anonymised data are information which does not relate to a living individual and cannot identify an individual, or does relate to a living individual but cannot identify an individual through other information which is in the possession of, or is likely to come into the possession of the organisation or person processing the personal data.

[4] If the person who needs these contact details can access them from OneDrive/SharePoint, then they should do so. If they cannot access them, consider whether they need to receive them at all.

		'protected characteristics'[5]
Simple list of names with no other personal data and not in a context which would be 'restricted' or 'highly restricted'	Name plus date of birth or national insurance number	Information on individuals which is classed under data protection laws as 'special category data'
Corporate contact details where the personal information is publicly available or does not identify an individual	Scan of identification documentation Dates of birth (without name)	Individual's name plus D.o.B and passport details, home address and telephone number
Information on individuals available through social network sites where information is provided on condition that will be in public domain	References for staff members not containing any 'highly restricted information'	Individual's name plus national insurance number and passport details, home address and telephone number[6]
Information contained in an organisation's annual corporate report	Meeting minutes which are not publicly published. They may include commercially sensitive information	Scan of identification documentation
Dates of birth (without name)	Funding applications/proposal	Misconduct or Disciplinary information

[5] Sometimes at Landward Research emails are sent around sharing the news of an individual's life step such as birthday, marriage, civil partnership or birth of a child / adoption. Under data protection laws these emails are personal data processing 'carried out by individuals purely for personal/household activities' and therefore do not count as 'restricted' or 'highly restricted'. If you do not want an email of this kind sent about you, you should inform your line manager.

[6] Combinations of personal data increase the risk of misuse of data / damage to the individual if received by the wrong person. E.g. a combination of personal details can increase the ability to carry out identify theft.

Information obtained from publicly available directories /regulatory bodies	Photos / film images taken by Landward Research, where someone is named or quoted	References for staff members containing 'highly restricted information'
Information on organisations' external websites	CVs (not containing date of birth or personal postal address)	Information relating to restricted intellectual property rights or covered by a confidentiality agreement/ contract[7]
Anything subject to disclosure under the Freedom of Information Act 2000	Information relating to supply / procurement of goods/services prior to approved publication	School children's personal information
Factual / general organisational information for public dissemination including annual reports or accounts	Documents containing signatures with the person's name legible including if the name appears typed on the document	CVs (containing date of birth or a personal postal address)
Meeting minutes which need to be published publicly. They will contain names and job titles, but these are already available in the public domain		Information that may be regarded as a trade secret or otherwise highly commercially sensitive
Photos / film images placed in the public domain by the data subject themselves (*i.e.* the person in the photo).		Legal advice and other information relating to legal action against or by Landward Research

[7] This is not personal data but is highly restricted and should be in a password protected attachment.

e.g. images they've put on a social media profile without privacy limitations (*i.e.* fully public profile)		
Photos / film images taken by Landward Research, where no-one is named or quoted		Documents containing signatures, name and another piece of personal data *e.g*. date of birth or address
		Landward Research business contracts if they contain commercially sensitive information (whether signed or unsigned)

If you require further advice, please contact the CEO via Kenneth.aitchison@landward.eu or 07803895033.