Unipol Student Homes
Data Protection and Information Security Policy 2024

1. Policy Statement

Every individual has rights in relation to how they information from which they can be identified (known as personal data) is handled. During the course of Unipol's business, we may collect, store and process personal data about our customers, staff and other third parties. This Policy also applies to Unipol's wholly owned subsidiary company, Leeds Student Homes.

Unipol Student Homes is committed to complying with the requirements of applicable data protection legislation including the Data Protection Act 1998 and the UK General Data Protection Regulation (UK GDPR), which are designed to protect the use of personal data from which individuals can be identified and to provide those individuals with certain rights.

The Policy and the Colleague Data Protection Handbook (collectively referred to as the Policy) sets out the principles which will must apply to processing of data to ensure we protected the data rights of individuals and process their data in accordance with data protection legislation.

1. Who Does this Policy Apply to?

This Policy applies to and must be complied with by all employees, workers, contractors, agents, and other third parties acting for or on behalf of Unipol (referred to collectively as Colleagues). This Policy forms part of the formal contract of employment. It is a condition of employment that employees will abide by this Policy and any failure to it can result in disciplinary proceedings. It is the responsibility of every colleague to ensure they understand the content of this policy and to seek guidance where any doubt exists. Those who work for Unipol as a contractor or consultant will also be expected to comply with this Policy insofar as they come into contact with personal data through Unipol and in connection with the provision of their own personal data.

2. Why do we have this Policy?

Ensuring personal data is handled correctly will support trust and confidence between Unipol and its customers and other third parties, and is key to business success. In addition failure to comply with data protection obligations could expose Unipol to enforcement action by the Information Commissioners Office (the ICO), including fines. Affected individuals may also complain or seek compensation, and any poor practice could lead to negative publicity.

3. Who is responsible for Data Protection?

All colleagues have a personal responsibility within their area of the business. Details of specific responsibilities within the business are below:

Board and Chief Executive

- Overall responsibility for ensuring compliance with the policy and Data Protection legislation

Data Protection Officer (The Company Secretary)

- Day to day responsibility for monitoring compliance with this policy including period spot checks and internal auditing activity
- Maintaining the Colleague Data Protection and Security Handbook

- Maintaining Unipol's Privacy Statement
- Provide support and guidance within Unipol on data protection matters including Data Protection Impact Assessments
- Receiving and actioning data requests such as Subject Access Requests
- Receiving and assessing data breach reporting
- Overseeing completion of required training
- Keeping abreast with changes in data protection legislation
- Reporting any data breaches to the Senior Management Team
- Review and update of this Policy
- To act as the point of contact for the ICO and to maintain Unipol's registration
- To provide an annual report on compliance with this policy

Seniors Management Team

- Ensuring that all systems, processes, records and datasets within their business areas are compliant with this Policy and with Data Protection legislation
- Assisting the Data Protection Officer with their duties
- Consulting the Data Protection Officer on new developments or issues involving the use of personal data and ensuring that Data Protection Impact Assessments (DPIA) are conducted as appropriate
- Ensuring their team have completed required data protection training
- Ensuring due diligence is conducted on suppliers/sub-contractors or third parties and ensuring data sharing agreements are in placed where required which specifies that the they agree to act on Unipol's instructions and to abide by the provisions of the Act in connection with data security.
- Ensuring team members retain data in accordance with the defined Retention Periods

All colleagues

- Responsible for complying with and understanding the Policy and all other procedures including reading and confirming their understanding of the Colleague Data Protection Handbook for the handling of personal data appropriate to their role
- Only collect and process personal data in accordance with the Purpose for which it is needed by Unipol to meet business needs or legal requirements
- Only access personal data they need to undertake their job and handle personal data in line with this Policy
- Ensure that personal data held by Unipol is accurate, complete and up to date
- Ensure that personal data is only retained for as long as necessary for the legal purpose for which is was obtained and that it is destroyed when it is no longer required in line with the Retention Periods in the Colleague Data Protection and Security Handbook
- Immediately notify the Data Protection Officer if there is an actual or suspected data breach
- Refer any data requests to the Data Protection Officer
- Complete annual training on data protection

In the event that colleagues have any questions in relation to this policy or concerns about compliance they can be raised with the Data Protection Officer on dataprotection@unipol.org.uk

4. Data Protection Principles

In processing personal data, Unipol needs to comply with UK GDPR which sets out 7 principles:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency')
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
4. accurate and, where necessary, kept up to date; every reasonable step must 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 ('accuracy');
5. 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');
6. 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 ('integrity and confidentiality').
7. The controller shall be responsible for, and be able to demonstrate compliance with the above ('accountability)

6. Rights of Individuals under this Policy

Under Data Protection Legislation, individuals have various rights to in respect of their use of their personal data including:

- Right to access for any data that is being processed, by submitting a Data Access Subject Request
- Right to erasure, by which an individual is entitled to request that any personal data held on them be deleted
- Right to rectification
- Right to restriction of processing
- Right for data to be transferred
- Right to object
- Rights related to automated decision-making including profiling (although Unipol does not currently make use of this technology)

Subject to certain exemptions, colleagues, students and others in contact with Unipol will on most occasions have the right of access to personal data held on them. This will normally be provided in the form of copies of the personal data or a report of the data held depending on the type and format of the original data.

Any person who wished to exercise this right should contact Unipol's Data Protection Officer on:

- Dataprotection@unipol.org.uk or 0113 243 0169

Individuals will normally be required to provide proof of identity and there is no fee payable for this service. However Unipol reserves the right to charge a fee, based on the administrative cost of providing the information, when a request is manifestly unfounded or excessive, particularly if it is repetitive or where the request is for further copies of the same information. Unipol will supply the information by loading it into a secure password protected downloads area of a Unipol hosted service and the data subject will be provided with a password for that area for a period of one month. It is illegal to dispose of personal data relating to an individual once he or she has lodged a written subject access request.

Unipol aims to comply with requests for access to personal information from data subjects as quickly as possible, but will ensure that it is provided within 30 days from the date of the request. However, if the request is complex or there are multiple requests from one data subject, Unipol may need extra time to consider the request and may take up to two further months for this. Unipol will conform if this is the case with the data subject within 5 days of receiving the request.

7. Complying with UK GDPR

Unipol has a Colleague Data Protection and Security Handbook that sets out how compliance must be achieved under this policy. This includes sections on:

- The Lawful Basis for Processing Personal Data
- Processing Special Category Data
- Accuracy of Personal Data
- Data Retention and Retention Periods
- Data Security
- Data Breaches
- Transferring Personal Data to Third Parties
- Transfers Outside of the UK
- Rights of Individuals under this Policy
- Data Protection Impact Assessments
- Direct Marketing
- Supplier Due Diligence

8. Privacy Statement

The Privacy Statement (included at Annex 1) details key information for tenants, external users of Unipol's services and third parties on how Unipol handles personal data.

9. Review of this Policy

Unipol's approach to data protection if kept under regular review through our wider compliance monitoring, and our approach will be adjusted and optimised based on this monitoring.

This Policy will be reviewed annually by the Data Protection Officer, with any changes approved by the SMT. It will be reviewed by the IT and Communications Committee on a biennial basis, and then approved by the Board.

Annex 1

Unipol Privacy Statement

How we handle your personal data is important to us; this page explains what personal data we collect, why we do this, how it is used and how we protect your privacy.

This information only covers external users of Unipol's services and websites, to find out how staff are protected you can read our data protection policy

If you have any questions about the information below or need help then you can email us at dataprotection@unipol.org.uk

Who we are

Unipol was established in 1975 and we provide help and assistance to students renting in the private sector, provide direct housing to students in Leeds, Nottingham and Bradford, run a number of accreditation schemes as well as training and promoting best practice in student housing.
We are a registered charity (no. 1063492) and company limited by guarantee (3401440) with our registered office at 15/157 Woodhouse Lane, Leeds, LS2 3ED, you can write to us at this address, email us at dataprotection@unipol.org.uk, or call us on 0113 243 0169.

Our data controller is Ms Victoria Tolmie-Loverseed who can also be emailed directly at dataprotection@unipol.org.uk.

Why we collect your data

We need personal information in order to provide four different types of service:

- Tenants of Unipol or those in properties managed by Unipol;
- Landlord services (which includes membership of the Unipol Codes and Leeds Rental Standard);
- Event booking;
- To provide house hunting assistance to students

We also collect it to help respond to enquiries, feedback and complaints submitted through forms on our websites, emails and web chat. Finally we use it to analyse and help improve our web services.

When is personal information collected

If you sign up for a Unipol service we will ask you to supply only information which is absolutely necessary to providing that service. We then log information, such as IP address and browser being used) each time you access our services and may ask for additional information while you are using

them. We record information given when you communicate with us through email, web chat or web forms.

We are provided with information on students and landlords from educational institutions for allocated tenancies and the Homestay service.

When you visit and interact with our websites we use Google Analytics and firewall logs to record information about your behaviour (what you click on) and demographic information such as gender, age and location. Although this may seem quite detailed there is no way for us to use this information to identify individuals.
Unipol collects and stores information on third party tenancies supplied from landlords using our tenancy agreement generator service.

What kind of data do we collect?

- Personal information you give when signing up and using a Unipol service;
- Personal information given to Unipol by an organisation where Unipol is providing a service in partnership with / for them;
- Contact details of trustees and others involved in governance;
- Feedback through our websites;
- Subscription information for news and service alerts;
- Booking details from people attending Unipol organised training and events;
- Payment transaction details – these do not include billing information such as card details which are processed for Unipol by a third party;
- Student to Student Noticeboard Messages and Rate Your Landlord reviewers;
- Information on people using our office wireless networks;
- Website usage and demographic information;
- Firewall and server logs of users accessing web services;
- Statistics on searches for accommodation which include filters used, results, viewing requests and personal clipboard lists or favourites

Where is your data held?

Most personal data is held either on Unipol's own servers or within 3rd party data centres both of which are located within the UK and this information is not backed up or transferred outside the European Economic Area (EEA). Only data from web chat is transferred outside the EEA and this is covered by the Privacy Shield Framework which ensures the data is handled in line with UK law.

How do we keep your data safe?

Our websites and services have numerous security measures in place to protect the loss, misuse and alteration of the information under our control. The measures include passwords, linkages to secure servers, encryption, data backup, and conventional locks and alarm systems. However we cannot guarantee that the measures in place are (or will remain) adequate.

How long do we keep personal data for?

Type of data	Length of retention	From
Tenant (direct and allocated)	7 years	Contract ending
Landlord	7 years	Service last used
Non-tenant student accounts	26 months	From last logon
Enquiries / web form entries	Maximum 26 months	From submission
Student to student noticeboard	90 days	From submission
Code Complaints	7 years	From submission
Payment transactions	7 years	From submission
Agreement generator	3 months	From submission
Google Analytics tracking information	26 month	From submission
Firewall and server event logs	12 months	From submission

Who has access to your information?

Within Unipol only staff who need to access your information to fulfil specific duties will be able to view and process it.

Where we work with third parties, some of who are based outside the EEA, to develop and support our services there are data protection agreements in place to make sure they access / process your data responsibly, only for defined reasons and in line with UK law.

Unipol will never sell or rent your information to third parties. We only share information with carefully selected third parties when agreement has explicitly been given.

If we have supplied an internet service as part of your tenancy this is done through a third party company and any personal information supplied during registration for this and during use of the service is subject to their privacy policies.

Requesting access to your personal data

You have the right to see any data Unipol holds on you, to do this submit a request to dataprotection@unipol.org.uk giving your name and what information you require. Unipol will respond within one month of the request or give reasons why the information cannot be provided within the month.

Your right to opt out

You can change your mind about receiving marketing information from Unipol and opt out at any time. This can be done by clicking the unsubscribe button on the bottom of the emails we send you, or if you have a user account, by logging on and changing your contact preferences. Your right to opt out only applies to marketing information.

We use technology called cookies to track your actions on our websites if you want to find out more about how this works and how to stop being tracked read www.aboutcookies.org

Your right to complain

You have the right to complain to the Information Commissioners Office (ICO) about how Unipol has handled your personal data you can contact the Information Commissioner at ico.org.uk/concerns/ or phone 0303 123 1113.

What happens when I link to another site?

Unipol may provide links to other websites; for example those of partner institutions, companies, government departments and other organisations. This privacy policy applies only to our sites, so you should always be aware when you are moving to another site and read the privacy statement of any site which collects personal information.

Detail in relation to certain Unipol Services

Unipol Tenants

Tenant Details
All tenants complete a Tenant Details form which contains a Data Protection Statement. Those tenants accepting a contract online are provided with the same statement as part on the Rent Online process. This highlights that information regarding a tenancy may be disclosed to joint tenants and statutory authorities, the deposit protection scheme that Unipol use and contractors who are carrying out work for Unipol. It also enables the tenant to provide the name and contact details of a third party with whom tenants agree Unipol can discuss details of the tenancy and or rent accounts. If the tenant does not nominate a third party at this stage they can provide written authorisation for this at any stage.

The Data Protection Statement reads as:
Data Protection Act 2018

By signing this form you are giving consent that any information given by you regarding your tenancy shall be processed and held by Unipol Student Homes. We will reasonably endeavour to protect the information we obtain from you from loss, misuse or unauthorised access leading to disclosure, alteration or destruction.

Information may be disclosed to joint tenants (in the case of you signing a joint tenancy agreement) and statutory authorities (including, but not limited to, local government agencies and to the police and other regulatory body where pursuant to the investigation or disclosure of a potential crime) on request. We will provide your personal details to close family and to the emergency services in the case of an emergency situations such as illness, serious injury or bereavement. We are required by law to protect any deposits collected using a Government-approved scheme. This will require us to disclose your details to the scheme administrators. We may disclose your name email address and telephone number to a Unipol-approved contractor, in order that they may contact you to arrange access to carry out a repair at your property. Unipol's out of hours security provider also has access to tenant details. We may disclose your name, address and contact details to research contractors for the purposes of conducting tenant surveys. In the event that you are in rent arrears Unipol may provide your details to an agent for recovery of the monies.

If a Third Party (i.e. parent, carer, local authority, guarantor) is paying your rent directly to Unipol by direct debit or on-line payment, then Unipol *may* disclose details of all your account to that person. However, Unipol will not discuss or disclose any information regarding your Tenancy to any Third Party claiming to represent you, unless you give us written permission to do so. You can do this here or you can do so at a later date by providing a signed letter of consent. If no letter is received, Unipol will not discuss any information regarding you with any Third Party.

[For students living in accommodation where Unipol has an arrangement with a University]

Personal information relating to your accommodation application will be transferred from your university as part of the allocation process. Full details of the data protection policies of these universities can be found on their websites.

Unipol may discuss any issue relating to my Tenancy with:
Name Address Daytime contact number Relationship to Tenant email address

Tenants and Finance
If a parent is paying the rent directly to Unipol then finance staff will be able to disclose to the parents details of the account. Tenants must provide a signed consent in order to disclose any other information (including deposit deductions) to parents or any third party. A standard letter giving permission for disclosure will be offered to tenants.

Tenants financial records
Finance staff keep records of former tenants who are in debt adding the agreements, tenants details forms and all correspondence to these files. The files are then retained for a period of seven years after the debt has been repaid. Files for these tenants will be kept separately from those tenants with no debts at the end of their tenancy.

When these files are destroyed the computer records for these tenants are also destroyed .

Unipol carries out due dilligence checks on tenants from specified high risk countries prior to entering into tenancy agreements, and retains the results of these checks for a period of seven years.

Tenants ID
Unipol are exempt as a charitable body estabilised for the purpose of housing students under the Immigration Act 2014 - Right to Rent. However when required to take copies of suitable documentation to prove identification and confirmation of the occupants right to rent for non students, this is kept in a separate electronic folder with limited access. Copies of the tenant's documents are retained for the time they are a Unipol tenant and for one year after.

Retention of tenants files
Tenants' correspondance files and supporting documentation including tenant details forms, correspondence files and agreements will be destroyed 7 years after the last correspondance with the tenant if the tenant no longer uses Unipol's services with the exception of the Right to Rent evidence.

Tenancy Support Case files
These files are kept for a period of 4 years since the case was closed.

Homestay
Details of the hosts and students and their profiles are kept for a period of 7 years.

Sensitive data

Data on tenants classified under GDPR as Sensitive may be processed for tenants for example in tenancy support cases when mental health or sexual life, criminal convictions etc may be raised. Anyone dealing with tenants must be made aware of the higher level of sensitivity placed on this type of data.

Tenant References

Tenants who want Unipol to supply a reference for them will give permission for data to be released in writing.

Tenants' Photographs

Unipol collect photographs of tenants in certain developments to provide proof of identity and to allow staff to more easily identify tenants captured on CCTV footage. We also take photographs at tenant social events.

Under 18's

Personal data regarding under 18 year olds may be disclosed to their legal guardian - details of which are kept on the Housing Management System.

Owners

Contact information

If an owner has chosen not to show their details such as address on the property advert this information cannot be released to anyone other than the agencies specified below. The owner has chosen that this information is not in the public domain. However, under Unipol's landlord registration we make clear that this information is available to statutory authorities including the Local Authority Housing Advice Service should they request it. They will most likely have the address in any event so if someone has a dispute with the owner they can be referred there. Staff will not give out this information without checking that the owner has agreed to this through the Advert options form on the owners database. As a minimum owners must agree to have a contact number in the public domain.

Owners are informed of Unipol Data Protection and Information Policy in relation to them on the Owners registration form.

Condition of Service states:

"GDPR - By registering to use this service, you are giving consent that any information given by you regarding your registration and any properties advertised shall be processed and held on systems operated by Unipol Student Homes and Leeds Student Homes Limited (our associated trading company). We will reasonably endeavour to protect the information we obtain from you from loss, misuse, or unauthorised access, leading to disclosure, alteration or destruction. Information may be disclosed to statutory authorities on request."

There is an opt out clause for the use of Unipol held data for marketing in condition of service:

"Unipol may also pass information to third parties for direct marketing purposes. Tick here if you wish to opt out from this."

Owners who have joined the Unipol Code sign the following clauses:

I/we understand that information about my Code status is in the public domain and will be accessible to all those using Unipol's web system and will remain accessible for up to three years regardless of my future membership of the Code

I/we accept that Unipol and its affiliated business partners including Nottingham City Council/Leeds City Council/Bradford Metropolitan District Council may use my personal information for the purpose of administering the Code, checking the suitability of landlords for accreditation including any criminal convictions, providing services, administration, and training and may disclose information to its service providers and agents for these purposes. If my personal details or the properties I/we own/manage changes I/we agree to inform Unipol.

Owners files

Registration forms and accommodation details forms are kept alphabetically in a lockable cupboard and are not accessible by the public. The records are also held electroncially.

Declaration forms for the Unipol Codes and ANUK/Unipol National Code of Standards for Larger Residential Developments are stored electronically or kept in a file in an office that is either staffed or locked.

Owners correspondance files are kept in individual files and then filed alphabetically in a locked filing cabinet that is not accessible to the public.

Managed Owners and Landlords

Due dilligence is undertaken on managed owners and landlords with rental income of £250,000 and over for compliance with client money protection schemes. The results of these checks are stored securely and can be destroyed 7 years after the date of their first collection.

Retention of Managed Owners and Landlord Files

Owners' registration and accommodation files can be destroyed after 7 years from the date of their last registration.

Owners' correspondence files will be destroyed 7 years after the last correspondence with the owner if the owner no longer uses Unipol's services.

Owners' financial information including tax information will be destroyed 12 years after the last correspondence with the owner if the owner no longer uses Unipol's services.

Owners online files will be lapsed after 7 years from their last registration."

Owners use of Tenancy Agreement Generator

These will be retained with tenant information for a period of 3 months from being completed and then they will anonymised so the owner can use the property information but Unipol is not holding personal data of the tenant.

Sensitive data

No data on owners classified under the DPA as Sensitive is processed for owners other than if raised as an issue in Code complaints when mental health or sexual life, criminal convictions race etc may be raised. Anyone dealing with Code complaints must be made aware of the higher level of sensitivity placed on this type of data.

Consultants

All consultants are appointed via a consultancy agreement and this makes clear the terms of that appointment. This includes standard clauses on data protection.

The Consultant is asked to consent to Unipol holding and processing data relating to him for legal, personnel, administrative and management purposes and in particular to the processing of any "sensitive personal data" (as defined in the Data Protection Act 2018) relating to the Consultant.]

The Consultant consents to Unipol making such information available to those who provide products or services to Unipol (such as advisers), regulatory authorities, governmental or quasi-governmental organisations and potential purchasers of Unipol or any part of its business.

Unipol Codes for Shared Student Housing, and ANUK/Unipol National Code of Standards for Larger Residential Developments

Owners in Leeds are asked to consent to information being transferred to Leeds City Council if they wish to join the Leeds Rental Standard.

Owners in Nottingham are asked to opt out of their data being shared with the Nottingham City Council and their accreditation agent for the purposes of joining the Nottingham Standard.

The Code database contains details of members of the Code and records of property inspections and access to this database is shared with, by written agreement, the relevant local authority.

Complaints will not be disclosed to a third party unless Unipol has the express permission of the complainant(s) concerned.

In agreeing to abide by the Codes, owners agree to the complaints and tribunal system. The minutes of the tribunal or chairs action are in the public domain and are placed on the website. The record relating to a complaint remains in the public domain for a period of 3 years from the date of the tribunal or chairs action.
All information disclosed to the Tribunal or in case of action by the Chair, to the Chair will be disclosed to the Owner.
A complaint made by a third party excepting where specifically allowed by the Codes is only acceptable with the express permission of the tenant/tenants concerned or those directly in a contractual relationship with the owner.
Paper records relating to the Codes are kept in an office that is either occupied or locked.

Information related to Code membership and tribunal decisions is in the public domain for three years and may be disclosed if appropriate for a further three years regardless of their future membership of the code.
The National Code of Standards for Larger Developments Codes are government approved schemes and as such data can be provided to Government (currently DLUHC) at their request.

Disclosures of Personal Data over the Telephone
Identity must be confirmed by home address and date of birth for tenants and reference number for owners.

Liaison with Other Agencies
Owners agree to the disclosure of personal information to statutory authorities upon request.

Owners Consultative Mailing List
The contact details of the Owners who are part of the Owners consultative group are available upon request by other Code owners.

House Hunting Events and Conference Bookings
House hunting participants will be informed on booking forms and confirmation details that their names and courses will be shared with other participants.

Conference delegates will be informed and confirmation details that their names and place of work or study will be shared with other participants.

Website privacy, Student to Student noticeboard and Unipol social media pages
Participants are aware that they are using a system in the public domain and can therefore leave their own contact details at their own risk and discretion. There will be a notice to this effect on both noticeboards and a privacy statement will be displayed on the main Unipol Web Site linked from the home page.

Housing Hub
House hunting enquiries sent by email will be kept for statistical purposes and deleted after 4 years. A report may be written around the stats but this will not identify any individual.

All other email from Unipol clients, contractors or partners can be deleted after 4 years. Email with ongoing relevance can be kept and may be printed out and filed in the appropriate paper file.

Outbound external emails contain the following message:
This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. No one else is authorised to disrtibute, forward, print,copy or act upon any information contained in this email. If you have received this email in error please notify the sended.

Applications for Jobs
In the Unipol job description/spec is included the following statement on Data Protection
“The information you provide in your application will be used to consider your suitability for the post for which you have applied. If your application is not successful the information will be disposed of confidentially 1 year from the completion of the application process. If your application is successful and you are appointed, your information and future data will be processed in accordance with the Unipol Data Protection Policy. A copy of this code can be obtained from the Unipol Website."

Version Control and Document Governance

Document Title	Data Protection Policy
Version	1
Level	IT and Communications Committee
Owner / Position	Victoria Tolmie-Loverseed – Company Secretary
Reviewed by	Victoria Tolmie-Loverseed
Approval	Unipol Board 26 September 2024
Review Period	Annually by SMT Two yearly review by IT and Communications Committee, approval by Board
Next Review	By DPO – June 2025 By IT and Communications Committee – June 2027
Publication	Policy to be published on the Unipol website Privacy Statement (Annex 1) to be published on Unipol website Colleague Data Protection and Security Handbook to be available internally