Unipol Data Protection and Information Security Policy
June 2018

Main Policy
Set out below is the Unipol's Data Protection and Information Security Policy, which accords with the GDPR and takes into account the codes of practice published periodically by the Office of the Information Commissioner.

Unipol's Data Protection Officer is Nikki Verity, the Company Secretary.

The code falls into two sections. The first, covered in paragraphs 1-49, constitutes a statement of general policy, which includes an indication of Unipol's obligations under GDPR. The second section, covered in paragraphs - 50-60, provides brief guidance notes for staff in connection with handling personal data.

There are four appendices to this document: Appendix 1: Processing Personal Data in Unipol – this forms the implementation plan for the policy and will be updated regularly; Appendix 2: Unipol Privacy Policy – to be put on the web site and linked from Unipol's front page, this informs Unipol's users how their data is dealt with; Appendix 3: Request form for access to personal data and Appendix 4 PCI DSS Cardholder Security Policy

Introduction
1. Unipol needs to process certain information about its employees, tenants, landlords and others. In so doing, Unipol must comply with GDPR.
GDPR sets out 7 principles:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

These principles should lie at the heart of Unipol's approach to processing personal data.

"(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

(b) 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');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) 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');

(e) 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');

(f) 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')."

Article 5(2) adds that:

"The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."

2. Some of the notable features of GDPRare that:

- It *places restrictions on what Unipol can do with personal data*; certain conditions, which include obtaining data subject consent, must be met before processing can take place. The term 'processing' covers almost anything that is done to data and the practical implications of these restrictions are wide-ranging
- It provides *access for staff and clients to personal data that relates to them.*

(There is *no entitlement to immediate or on-site access* but the Act places a responsibility on Unipol to respond to access requests in good time. To this end all data subject requests will be handled centrally by the Company Secretary.)

- It places emphasis on data security, especially in relation to the unauthorised disclosure of personal data to third parties.

3. Unipol and all staff or others who process or use any personal information must ensure that the data protection principles and the laware followed and fully implemented

In order to facilitate this, Unipol has developed a code of practice on data protection which is a derivative of the University of Leeds' Code and Leeds Beckett University's Code. The references to personal data made within this document apply to all data held on any living individuals within Unipol, not just clients and staff.

Status of the Policy

4. 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.

5. 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.

What are personal data?

6. Personal data is *information about a living individual, who is identifiable by the information, or who could be identified by the information combined with other data*, which Unipol has or may have in the future. This includes names and addresses, features such as hair and eye colour - which will often be in the form of photographs - ethnic origin, qualifications and experience, details about staff sick and annual leave, dates of birth or marital status. Furthermore, any recorded *opinion about* or *intentions regarding a person* are also personal data.

7. The Act covers ALL personal data held in Unipol, irrespective of whether this is held by individual members of staff in their own separate files or in a central store or filing cabinet.

8. The Act distinguishes between *ordinary* personal data such as name, address and telephone number and *sensitive* personal data including information relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric dates (whre this is used for identification purposes, health data, sex life or sexual orientation. Personal data can include information relating to criminal convictions and offences. . The processing of sensitive data is subject to much stricter conditions. In particular processing of sensitive personal data requires explicit consent. While the Act permits the processing of data without consent where this is for the legitimate activities of Unipol and is not to the detriment of individuals, in most instances consent to

process ordinary and sensitive data is obtained routinely by Unipol for the avoidance of doubt. (see paragraphs 12-14 below and Appendix I).

Electronic and manual data
9. Almost anything that is done to data, namely, collection, use, storage and retention by reference to individuals is generally covered by the Act.

10. Personal data within emails, letters and hand written notes are covered.

11. In practical terms, however, it is seems prudent to assume anything recorded relating to and individual may fall under the provisions of GDPR.

Subject Consent
12. In many cases, Unipol can process personal data only with the consent of the individual. In some cases, if the data is sensitive, explicit consent must be obtained. Unipol has a duty, under certain circumstances, to ensure that staff are suitable for the job. On occasion it will be necessary to carry out independent verification of criminal records. Where this is relevant to the job, Unipol may also ask for information about particular health circumstances
13. As noted in paragraph 8 above, in most instances staff will not need to consider whether consent is required or to obtain consent to process from data subjects because such consent is obtained routinely by Unipol and jointly with the University of Leeds for staff. All applicants for employment, tenancies or owner who use the service are asked to signify their consent for processing both ordinary and sensitive personal data on application for the purposes on processing that application. Upon tenancy sign up, acceptance of any offer of employment, registering with the Unipol Code or to use the advertising services, students, owners and staff are asked to give consent to processing a wider range of data. Agreement to Unipol/the University of Leeds processing of this personal data is a condition of acceptance into a tenancy, a condition of advertising on the website/ Hub membership or of Code membership and a condition of employment for staff; a refusal to provide consent may result in discontinuation of the application. Further information on this point is set out in Appendix 1 of this code of practice.

14. Consent to process the personal data of external inquirers or other users of Unipol's services will be unnecessary in most instances as Unipol can rely on the provision within GDPR for processing under the lawful bases for processing.. However if personal data relating to external individuals is to be used subsequently for purposes other than the original enquiry (for example in creating a database to be used in advising individuals about Unipol's services) consent should be obtained as a precaution.

Retention of Data
15. It is not in the interest either of data subjects or of Unipol to retain unnecessary or duplicative information. It is Unipol policy to discourage staff from retaining personal data within files for longer than it is needed and staff will follow the guidelines for the retention of personal data set out in the staff guidance notes. Unipol does, however, retain some data relating to former staff and clients - most of which is held in the Unipol Archive or in the case of staff the University of Leeds archive - partly in order to comply with statutory requirements but primarily as a way of maintaining a complete historical record.
Guidelines for the retention of personal data are set out in Appendix I to this code of practice

Access to data
16. Subject to certain exemptions, staff, students and others in contact with Unipol will on most occasions have the right of access to personal data held on them (see footnote note 2).. 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 complete Unipol's data access request form and forward it to the Company Secretary with the required proof of identity. There is normally no charge for dealing with a subject access request. 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 wihll 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.

17. 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.

Staff obligations

18. In addition to their responsibilities for processing personal data about tenants,conference delegates, students andandlords (and in some instances, colleagues), staff are also data subjects in their own right. In connection with personal data on clients and colleagues, *all staff must comply with Unipol guidelines on data protection*.
Unipol cannot carry out its legal responsibility to maintain up to date personal data unless staff

- ensure that any information that they provide to Unipol in connection with their employment is accurate and up to date
- inform Unipol of any changes for which they are responsible, for example, changes of address (Unipol cannot be held accountable for errors arising from changes about which it has not been informed).

19. Staff who supervise contractors, consultants who come into contact with personal data are responsible for drawing their attention to this Code of Practice.

Any request for information by a third party should be referred to the Company Secretary.

20. Client obligations
Owners, students and others who access Unipol's services must ensure that all personal data provided to Unipol is accurate and up to date - Unipol cannot be held accountable for errors arising from changes about which it has not been informed. Unipol is obliged to correct any inaccurate information held once this has been provided by the data subject.

Data Security

21. All staff must adhere to the University policy and guidelines on data security, including the University's Information Protection Policy. Generally staff must ensure that:

- any personal data which they hold is kept securely
- personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.

22. Staff should note that unauthorised disclosure may be a disciplinary matter, and could be considered gross misconduct in certain cases.

23. Staff must ensure that, where a data processor, contractor or company engaged by Unipol processes data on Unipol's behalf (a mailing agency, or IT support company for example) there is a Data Protection Agreement between the parties which specifies that the processor agrees to act on Unipol's instructions and to abide by the provisions of the Act in connection with data security.

24. Staff should make reasonable efforts to ensure that all personal information is kept securely but should pay particular attention to the security of sensitive data. All personal data should be accessible only by those who need to use it and sensitive data must be either:

- kept in a lockable room with controlled access or
- kept in a locked filing cabinet, or
- in a locked drawer, or

protected by password if held on a computer kept only on disks which are themselves kept securely
25. Care must be taken to ensure that PCs and terminals are not visible except to authorised staff and that computer passwords are confidential. Screens should not be left unattended when personal data is being processed and manual records should not be left where they can be accessed by unauthorised staff. When manual records are no longer required, they should be shredded or bagged and disposed of securely; and the hard drives of redundant PC s should be wiped clean.

26. Off-site use of personal data presents a potentially greater risk of loss, theft or damage to personal data; and the institutional and personal liability that may accrue from the off-site use of

personal data is similarly increased. For these reasons staff and others, including members of the Unipol Board:

- Should take personal data off site only when absolutely necessary, and for the shortest possible time, especially where sensitive data is being processed
- Should take particular care when laptop computers or personal machines are used to process personal data at home or in other locations outside Unipol.
- Should be aware of this code of practice and their responsibilities under it apply when data are processed off-site
- Should note that Board Papers are confidential to board members and fall within the parameters of data protection, information security and commercial confidentiality. Papers include confidential matters regarding tenants, staff and some commercial matters and are highly sensitive. Whilst board minutes are available to the general public as part of the accountability of the charity, those minutes are written in a particular format to address the maintenance of confidentiality including arrangements for Confidential Minutes to record material that cannot be on open access.

Publication of Information

27. It is Unipol's policy to make as much information public as possible; in particular the following information may be available publicly:

- lists of staff
- names and work contact information of staff
- email addresses
- photographs of staff
- profiles of staff

28. It is of course a condition of employment that staff consent to the processing of their personal data. Nonetheless, it is recognised that there might be occasions when a member of staff or student has good reason for wishing details in these lists or categories to remain confidential or to be restricted to internal access, in which case they should contact the designated data contact. It is understood that this is especially the case in connection with the publication of photographic images of staff, particularly on web pages; all members of staff are advised that such images should not be made publicly accessible without the consent of the individuals concerned.

Monitoring of communications and use of CCTV

29. Unipol must ensure that its resources are not abused or used illegally for example accessing pornographic material on the worldwide web. Unipol may from time to time monitor staff communications without giving notice. Random monitoring or personal computer usage will only apply to publicly accessible computers and random monitoring of phone calls will not take place.

In any case:

- Any monitoring will be carried out only by a limited number of staff
- Personal data obtained during monitoring will be discarded as soon as possible after the investigation is complete
- Staff involved in monitoring will maintain confidentiality in respect of personal data.

30. For reasons of personal security and to protect Unipol premises and the property of tenants and staff, and to ensure that Unipol's resources are not abused closed circuit television cameras are in operation in certain locations. There are occasions when, to ensure the effectiveness of this surveillance, the presence of these cameras may not be obvious. Wherever CCTV images are being recorded there will be a notice stating this giving the Unipol telephone number for contact. In certain developments CCTV images are transmitted through the television distribution system so that tenants can monitor the security of common areas themselves. Tenants in such developments should be reminded that images are for their own personal use.
In some locations the images of security cameras are on public display on large screens.

31. A number of areas of Unipol use webcams and the data is transmitted over an internet connected network. Network security precautions are taken, however there is a risk that the images of individuals could be transmitted worldwide and a warning sign is posted within the area covered by the webcam.

32. Tenants or staff who consider that the positioning of a closed circuit television camera or use of a webcam is inappropriate should contact theCompany Secretary.

World Wide Web and Email
33. The provisions of the Act apply as much to web sites and to email as they do to data processing by any other means; *any* personal data downloaded from the web, included within a web site, or contained within an email are subject to the same restrictions as information held in manual files or on databases. In particular:

- authors of web pages should be aware that information posted onto a web page is potentially accessible world-wide (unless access is restricted in some way): the type of data placed onto web pages should reflect this.
- staff sending emails that include personal data on third parties should be confident that confidence and security will not be breached by the recipient, and they may wish to consider the use of encryption or other security measures. In most cases Unipol will use the secure download area of the web.
- staff setting up a web page or site which involves processing personal data – including the creation of mailing lists – will seek consent to process the data from the Company Secretary and abide by Unipol's privacy statement.

Cross-border data flows
34. The Act places restrictions on the transfer of personal data outside the European Economic Area, unless the country or territory involved ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. If, after careful consideration, it is regarded as essential that the transfer of personal data outside the EEA should take place - and if the transfer does not qualify as one of the circumstances when this principle does not apply - the consent of the data subject must be sought. Members of staff should note that this restriction has particular implications for international research projects and information placed onto web sites.

Research data
35. Personal data processed only for research purposes receive certain exemptions where the data are not processed to support measures or decisions with respect to individuals, and where no substantial harm or distress is caused. In essence, such personal data:

- can be processed for purposes other than for which they were originally obtained
- can be held indefinitely
- are exempt from the data subject right of access where the data is processed for research purposes and the results are anonymised.

36. The Act does not give blanket exemption from all data protection principles for data provided and/or used for research purposes. Most of the principles apply (notably the requirement to keep data secure); and staff will need to assess the legality of processing on each occasion that data are provided for research purposes. Furthermore, staff conducting research will need to ensure that:

- data subjects whose personal data will be used in research are advised as to why the data is being collected and the purposes for which it will be used
- a suitable mechanism is in place to ensure that data subjects can meaningfully exercise their right to object to the processing of their data on the grounds that it would cause them significant damage or distress
- particular care is taken when the processing involves sensitive personal data for which stricter conditions apply, including the need to obtain explicit consent for processing.

37. Finally, staff conducting research involving the processing of personal data must do so in the context of any ethical guidelines or codes of practice particular to their field of study; and it may be necessary to confirm the compatibility of such codes with GDPR.

Confidential references
38. For practical purposes staff must assume that Unipol can no longer guarantee confidentiality in respect of references received by Unipol or expect those we provide will remain confidential. Where Unipol request a reference there is a clause making clear this policy.
39. Where a data subject request is lodged by an individual, Unipol will need either to obtain consent to disclose any references covered by the request or to disclose references in anonymous format. If a

person wants a reference from Unipol they must make a written request. References will only be provided by the Chief Executive or the Deputy Chief Executive.

40. Explicit consent must always be sought from the data subject where references are provided for organisations located outside the EEA

The Unipol Codes, and ANUK/Unipol Code of Standards for Larger Residential Developments
41. 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 membership status at that time. The National Code of Standards for Larger Developments Codes are government approved schemes and as such data can be provided to Government (currently MHCLGMHMHCLG) at their request.

Complaints
42. Any member of staff or a client:

- who wishes to raise concerns or complain regarding the processing of his or her personal data should contact the Company Secretary in order to discuss the options for resolving their concerns.
- who considers that the policy has not been followed in respect of personal data should raise the matter with the Company Secretary. If the matter is not resolved with the help of the Company Secretary it should be raised with the Chief Executive.

Conclusion
43. Compliance with GDPR is the responsibility of all members of staff at Unipol. Any breach of the Data Protection and Information Policy may lead to disciplinary action being taken or even a criminal prosecution by third parties. Any questions or concerns about the interpretation or operation of this policy should be taken up with the Company Secretary.

Further information
44. Data protection is a complex area and in addition to the brief guidance notes set out below, further information is available to staff from the following sources:

- Unipol's designated data contact - the Company Secretary.
- Regular data protection bulletins, which will be circulated to senior managers who will disseminate to other staff.
- The Information Commissioners Office Website www.ico.gov.uk

GUIDANCE NOTES FOR STAFF

45. In addition to their responsibilities for processing personal data about clients (and in some instances, colleagues), staff are also data subjects in their own right. Most staff process personal data about tenants and landlords on a regular basis. Some staff frequently also process information about other staff, especially in the context of recruitment and internal procedures, including those for promotion, disciplinary matters and appeals.

46. Unipol ensures that all clients give their consent to processing ordinary and sensitive personal data *via* registration procedures, and that they are notified of the categories of processing as required by GDPR..

47. Consent to process ordinary and sensitive personal data has been sought from individual members of staff appointed from February 2001. Staff appointed before this date are deemed to have given their consent.

48. Where exceptionally consent to process personal data has been sought from external individuals the following phrases will be used
Enquiries made over the telephone or in person
“May we assume that you are content for Unipol to use your personal data (by which we mean your name and address) to provide you with information about our services?”
Enquiries generating written correspondence:
“Unless you advise us to the contrary we will assume you are content for Unipol to use your personal data (by which we mean your name and address) to provide you with information about our services.”

49. All staff have a duty to make sure that they comply with the data protection principles, which are set out in Unipol's Data Protection and Information Policy. In particular, staff must ensure that records are:

- accurate;
- up-to-date;
- fair;
- kept and disposed of safely, and in accordance with Unipol's policy.

50. Senior Managers i.e. Chief Executive, Deputy Chief Executive, Director of Finance, Assistant Chief Executive - Housing , Assistant Chief Executive Communications and IT, Assistant Chief Executive Standards, and Assistant Chief Executive- Hub are the only staff authorised to hold or process sensitive data.

51. All staff, including non-contracted staff, will be responsible for ensuring that data is kept securely.

52. Staff must not disclose personal data to a third party unless reasonable steps have been taken to verify the identity of the third party *and*

- the landlord, member of staff or student concerned has given consent to the disclosure, *or*
- approval has been given by a member of the senior management team *and*
- disclosure is in the best interests of the student or member of staff or a third person, or is otherwise urgent and necessary in the circumstances, or is required in compliance with the law.

53 Third party disclosure under the final bullet point of the previous paragraph should occur only in very limited circumstances (for example, if personal data is required urgently where a member of staff or student is injured and unconscious, but in need of medical attention).

54. Where disclosure is requested by the police, the matters should be referred to Nikki Verity, the Company Secretary, (on 0112 205 3431) or Rachel Campey, Assistant Chief Executive - Housing Services (on 0113 205 3405). Outside office hours contact with these individuals can be made via Unipol's out of hours service (0113 244 3799).

55. Where a member of staff is in doubt about how to proceed on third party disclosure, he or she should contact either the Company Secretary or the Chief Executive.

Staff Checklist for Processing Data

56. Before processing any personal data, all staff should consider the checklist set out below.

- do you really need to record the information?
- is the information 'ordinary' or is it 'sensitive'?
- does Unipol have the data subject's consent?
- are you authorised to collect/store/process the data?
- if so, have you checked with the data subject that the data is accurate?
- are you sure that the data is secure?
- if you do not have the data subject's consent to process, are you satisfied that it is in the best interests of the client to collect and retain the data?

Access requests

57. The Act gives individuals the right to access data held about them by Unipol. However, this is not an entitlement to immediate access - Unipol has thirty days in which to comply with data subject access requests - and *staff should forward all such requests to the Company Secretary.*

58. The Act also means that any recorded *opinion about* or *intentions regarding a person* are also personal data to which a data subject may gain access. This should be borne in mind when written or other records are made (and this includes emails and audio recordings, in addition to computer and manual files) and when files are weeded for unnecessary or duplicative material. The following is a useful test to apply to 'doubtful' comments:

- Is this comment fair, accurate and justifiable?
- Would I feel comfortable showing this to the data subject?

If the answer to the question - and in particular the first question - is 'No', then the comment should go unrecorded.

59. Access rights also mean that the confidentiality of references provided either internally or for external bodies can no longer be assumed. Again, this should be borne in mind when references are drawn up and in general terms the information provided in references should:

- confirm the accuracy of or provide factual information
- differentiate between statements of fact and opinion
- express only justifiable opinions, based on first-hand experience
- be fair and accurate
- avoid ambiguous or coded language.

60. All staff should ensure that inappropriate data are neither recorded nor retained. Once a data subject has requested access, the law specifies that data relating to him or her must not be 'weeded'.

Cross-border data flows

61. Staff must take special care in connection with requests for the transfer of personal data outside the European Economic Area. Staff should refer any such requests to the Company Secretary. In particular, staff should not:

- disclose personal data requested by non-EEA governments, agencies and organisations for the purposes of assessing the names, numbers and whereabouts of foreign nationals studying overseas without the specific and informed consent of the data subjects concerned
- disclose personal data requested by non-EEA governments for the purpose of determining liability to attend National Service, without the specific and informed consent of the data subjects concerned.

Further information

62. Further information and advice is available from the Company Secretary.

Footnotes

1. GDPR does however, permit the processing of data without consent were this is for the contractual, legal legitimate interests and activities of an organisation and is not to the detriment of the individuals.

2.This right will not for example, apply to documents regarded as being within the ambit of 'legal privilege', that is, those setting out legal counsel and related correspondence; and where access may disclose personal data related to a third party who has not consented to such disclosure (in respect of confidential references for example.

Unipol Data Protection and Information Security Policy
Appendix 1: Processing Personal Data in Unipol

Tenants
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 1988

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 your deposit 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 also disclose your name, property address and contact details to a partner agent, Let Leeds, in order for them to contact you to arrange a viewing of your property with a potential new tenant. 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, Unipl will not discuss any information regarding you with any Third Party.

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

Leeds Beckett Allocated Tenants
Leeds Beckett allocated tenants are provided with the following information

Data Protection Act 1998

By accepting this offer of accommodation, you are giving consent that any information given by you regarding your accommodation application shall be processed and held on systems operated by Unipol Student Homes. Unipol will reasonably endeavour to protect the information obtained from you from loss, misuse, or unauthorised access, leading to disclosure, alteration or destruction. Information may be disclosed to statutory authorities on request.

Please note that if a third party (e.g. a parent) is paying your rent directly to Unipol by standing order, direct debit on online then by agreeing this, you are giving consent that Unipol may disclose details of all your account to that person.
If you would like any other third party to act on your behalf in relations to matters surrounding your tenancy with Unipol, you must provide a written signed letter of consent so that we are able to

disclose any other information to them. If no letter is received then Unipol will not discuss or disclose any information regarding you to any third party claiming to represent you. This letter should be sent to Unipol Student Homes, 155 Woodhouse Lane, Leeds, LS2 3ED, and should clearly identify you as the tenant as well as the names of all third parties you nominate to act on your behalf.
Personal information relating to your accommodation application will be transferred from Leeds Beckett University to Unipol Student Homes, as part of the allocation procedure. (Leeds Beckett's full Data Protection and Information Policy can be found on their website, www.leedsbeckett.ac.uk.)

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 .

Tenants ID
Unipol are expempt as a charitable body establised 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.

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

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 data protection registration 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 number “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 may use my personal information for the purpose of administering the Code, 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 Codesand ANUK/Unipol Code of Standards for Larger Residential Developments are 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.

Retention of owners 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
The Consultant consents 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 1998) 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.

Consultants shall only have access to data held by Unipol that is specifically relevant to the work they carry out and this shall be decided at the outset of the Consultancy. Within the Consultants agreement is a clause about data protection as follows:

COMPANY POLICIES

The Consultant agrees to Unipol's general employment policies, including but not limited to those policies relating to health and safety, data protection and diversity as found on Unipol's web pages and as amended from time to time.

Unipol Codes for Shared Student Housing, and ANUK/Unipol 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 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 DevelopmentsCodes are government approved schemes and as such data can be provided to Government (currently MHCLG) 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 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.

Clear Desks and Screens
Staff whose offices have open public access in the Housing Huband areas close to Meeting Rooms will ensure that files that contain personal data will be secured at night and no files with personal data are left on desks when unattended.
Staff Computers should be locked when unattended and where possible, should be positioned so that personal information on screen is not visible to onlookers. Where this is not possible discretion should be used when viewing personal information on screen avoiding viewing when there is a risk that the screen can be viewed by others.

Dealing with the Press
Unipol will not release any personal data that is not in the public domain to the press without the express permission of the person concerned.

E-mail Messages
Emails containing personal data (this may include personal email addresses) will not be forwarded to another organisation without the express permission of the sender. Moreover, when such referrals do occur, the sender will be given details on each occasion.

BCC should be used on mailings to protect the identity of members of mailing lists.

Housing Hubhouse 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 distibute, forward, print,copy or act upon any information contained in this email. If you have received this email in error please notify the sended.

Staff Training on Data Protection
This policy will be included in the checklist for staff induction. All staff will receive training with their induction.

Monitoring
Line managers will ensure that this policy is carried out. TheCompany Secretary will have overall responsibility for this area. The policy will be reviewed annually by the Board.

Unipol Staff
Unipol Staff are jointly employed by the University of Leeds (‘the University’). Unipol processes staff personal data in line with the University of Leeds Data Protection and Information Policy.

Introduction

The data for which consent to process may be considered as having been obtained are set out below. Staff who wish to process personal data not included in these extracts should obtain consent from the data subject(s) first; and should also contact the Company Secretary.

Use of Staff Personal Data
Unipol and the University wishes to make it clear to all members of staff and other workers how Unipol and the University will process their personal data (including certain sensitive data). In essence, in order to function normally, the University needs to process 'ordinary' and 'sensitive' personal data for employment-related purposes. Processing of certain data will for some activities continue after individuals have left the service of Unipol and the University.
The list shown below does not preclude the Unipol and University from processing personal data that is included within its registered use under the Data Protection Act or in any other way allowed under the law.

All members of staff and other workers agree to the University and Unipol processing their personal data for the following purposes: -
1. Payment of salary, pension, sickness benefit or other payments due under the contract of employment.
2. Monitoring absence or sickness under an absence control or capability policy.
3. Training and development purposes.
4. Management planning.
5. Providing and obtaining references and consultation with external agencies, including police checks where necessary for the purposes of employment *for job applicants and employees in post; and providing references for former employees.*
6. For disclosure to the police or other regulatory body where pursuant to the investigation or disclosure of a particular crime.
7. Promotion and salary progression exercises.
8. Negotiations with trade unions or other staff representatives
9. Curriculum planning and organisation.
10. Time table organisation.
11. Administration of University codes of practice and policies.
12. Compliance with equality legislation including that relating to disability..
13. Compliance with any statutory or legal requirement to provide information about staff or other workers including, for example, statistical returns to external bodies and staff membership lists to Unions.
14. Administration of the University's disciplinary and grievance procedures.
15. Direct mailing for third party services reasonably concerned with employment-related matters or staff benefits.
16. Production of published staff lists including the University Calendar and telephone and e-mail directories for both internal and external use.
17. Production of Staff Identity Cards.
18. Production of photographs of staff for display within the University/Unipol or on the web.
19. Development of staff research profiles by associated University companies.
20. Monitoring the use of University and Unipol resources. This may include accessing email accounts and data during unexpected staff absence and post employment (subject to formal authorisation and controls)
21. In relation to the safety of individuals and their property and the protection of University assets, including the use of CCTV.
22. In relation to the provision of academic services and other services (for example, car parking).
23. In relationship to membership of University and staff clubs, societies and similar organisations.
24. For disclosure to close family and emergency services in the event of an emergency, for example, illness, serious injury to the member of staff or bereavement.25. In relation to exit questionnaires distributed to those leaving the University of Leeds or Unipol's employ.
26. In connection with data processed by external contractors or consultants from whomUnipol may obtain services or seek advice.
27. For disclosure to Data Processors who are registered under the Data Protection Act in order for them to process data on behalf of the Unipol or the University of Leeds for any of the purposes for which the Unipol or the University of Leeds is permitted to process the data, including the provision of academic and other services by the University or Unipol.

28. For disclosure to the University of Leeds or Unipol's insurers in respect of accidents occurring within the institution and to the University's external auditors.

29. The dissemination of staff contact details for use in connection with critical incident management plans.

30. The disclosure to trade union of University/Unipol staffs' names, category (e.g. academic other related or clerical) and relevant service together with such other personal data as the University may think appropriate in serving good industrial relations.

Unipol follows the guidelines for retention of personal data as outlined in the University of Leeds policy.

Guidelines for Retention of Personal Data

Type of Data	**Maximum retention period**	**Reason for Length of Period**
Personnel records for staff subject to below	6 years from the end of employment	To allow for completion of references
Application forms and interview notes for unsuccessful candidates	1 year for completion of the appointment process. (Successful job applicants documents will be transferred to the personell file and retained as above)	Possibility of legal challenge. 6 months normal max but with possibility of grounds for extension 1 year is sensible.
CRB check documentation	6 months from completion of appointment process	Period to deal with any request for feedback/challenge from applicants. 6 mnths max set by CRB
HR records of staff identified to be of archival interest following archival management process -Senior staff in named positions only	Indefinite	Of indefinite use for research purposes
Pension		
PAS members - member contributions paid, unpaid absences, maternity leave absences, salary history, and part time service fractional changes. Any correspondence & calculations of benefits on leaving or retirement, or on transferring benefits into PAS	Up to staff's death	Purposes of calculating and verifying benefits
USS/NHS/TPS members - member contributions paid, unpaid absences, maternity leave absences, salary history, and part time service fractional changes.	Up to 12 years after the person leaves the University's employment, retirement or death (whichever is earlier)	Purpose of calculating and verifying benefits.
Facts relating to redundancies where less than 20 redundancies	3 years from the date of redundancy	As above
Facts relating to redundancies where 20 or more redundancies	12 years from date of redundancies	Limitation Act 1980
Income Tax and NI returns, including correspondence with	At least 3 years after the end of the financial year	Income Tax (Employment) Regulations 1993

tax office	to which the records relate	
Statutory Maternity Pay records and calculations	As Above	Statutory Maternity Pay (General) Regulations 1982

Statutory Sick Pay records and calculations	As Above	Statutory Sick Pay (General) Regulations 1982
Wages and salary records	6 years	Taxes Management Act 1970
Accident books, and records and reports of accidents	3 years after the date of the last entry	Social Security (Claims and Payments) Regulations 1979; RIDDOR 1985
Health records	During employment	Management of Health and Safety at Work Regulations
Health records where reason for termination of employment is connected with health, including stress related illness	3 years	Limitation period for personal injury claims
Medical Records kept by reason of the Control of Substances hazardous to health Regulations 1994	40 years	Control of Substances Hazardous to Health Regulations 1999
Ionising Radiation Records	At least 50 years after last entry	Ionising Radiations Regulations 1985
Landlords records and tenants records	7 years after the end of using Unipol's service or after the last correspondence or after having cleared a Unipol debt. 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.	Time limits on litigation
User of the website databases	3 years from the last login	

As staff are on joint contracts the University policy for processing of staff personal data, including the use for marketing, is relevant.

Staff Records
Contact details given by staff to line managers. This should be kept by them in a place that is only known and accessible to Senior Managers.

Staffing files keeping all records or correspondance between the staff, University and Unipol is kept in the cabinets in the Chief Executive's Office and the Deputy Chief Executive's area. This is only accessible by the Senior Managers i.e. Chief Executive, Deputy Chief Executive, Assistant Chief Executive Communications and IT, Director of Finance, Assistant Chief Executive - Housing , Assistant Chief Executive - Standards, the Assistant Chief Executive- Hub , the Office Adminstrator and Homestay Coordinator and the person whose file it is. A check may be done on the file before access is granted to ensure that no personal data relating to another member of staff is in there. If there is such information this is not accessible by the member of staff.

Staff Computer Records
Are stored in the Staffing, Chief Executive's or the Deputy Chief Executive's electronic directories all of which have restricted access. This is only accessible by the Senior Managers i.e. Chief Executive Deputy Chief Executive, Assistant Chief Executive Communications and IT, Director of Finance,

Assistant Chief Executive - Housing, the Assitant Chief Executive Standards and the Assistant Chief Executive - Huband the Office Administrator and Homestay Coordinator.

No staff should keep personal data including addresses on any staff beyond the life of the document e.g interview letters for mailout will be deleted from the working file once they have been stored in the restricted access directories.

Staffing Matters are reported to Unipol Board
The staffing sections of the agendas and minutes of the Financial Affairs and Staffing Committee agendas are confidential to Board members and members of the Financial Affairs and Staffing Committee. The staffing minutes from the Financial Affairs and Staffing Committee are kept in a separate file from the Board papers and stored in the Chair's and Chief Executive's Office and are accessible by the Senior managers and Board members, on request.

Attendance and Sickness Records
No attendance and sickness records should be on public view. Staff holiday records are kept on a computerised calendar for staff consultation. Staff sickness records are kept in a locked filing cabinet or drawer and all computer records must be in a password protected directory. A computerised calendar of staff sickness is maintained and is accessible by the Senior Managers.

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 ProtectionPolicy. A copy of this code can be obtained from the Unipol Website."

Staff References
Unipol cannot guarantee confidentiality in respect of references received by Unipol or expect that those we provide will remain confidential.
In a Unipol request for reference we state:
"Under the Data Protection Act the applicant will be able to see the reference that you provide. Can you therefore please assume that your comments will not be confidential."
Staff who want Unipol to supply a reference for them will give permission for data to be released in writing.

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

Staff Personal E-mails and Phone Calls
Staff should not use their Unipol E-mail address for personal E-mails but in the event that they do they should be aware that all emails are accessible and viewed by Senior staff. This is essentially to ensure that email is answered in a member of staffs absence however it may be monitored by the Communications and IT Manager for misuse.

Unipol reserves the right to inspect the contents of any emails that staff send or receive. Inappropriate use of email could result in disciplinary action.

Photographs
Permission will be sought if Unipol wishes to publish photographs of individuals whether staff or students. Photographs of unidentified persons engaged in anti-social behaviour may be captured from CCTV and put on display for identification. Once identified these photographs or individuals on these must be removed from display.

Computers
Under GDPRUnipol has to ensure that all data is secure. All non-temporary staff have individual usernames and passwords and are informed that under no circumstances should this be shared with anyone else.. No paper or computer notes of any passwords must be kept apart from those for

generic user accounts kept by the Assistant Chief Executive - Communications and IT and the ICT Officers.

Staff are informed that they must not allow anyone to inadvertently have access to personal data by leaving their screen on and your computer unattended and unlocked. Guest access to Unipol computer facilities must be in a supervised area and care should be taken that guests do not access personal data.
Staff are reminded that Unipol computer resources are not for personal use. Staff should be aware that any personal documents that are on the computer can be accessed by other staff through the shared directory system. No staff, other than senior managers are allowed to attach a password to a document restricting access without permission from a member of the Senior Management Team.

Only authorised devices are permitted to access Unipol's core network and this access is controlled by Active Directory policy, IP address assignment and Firewall configuration.

Cloud storage
Staff should notify IT of any accounts created to use these services and access must only be through a Unipol email address.

These services must not be used to store or process data which is confidential or commercially sensitive. It should also not be used to store single copies of data that could adversely affect functions or operations of Unipol would be disrupted should it be lost or become unavailable or corrupted.

Social Media
Creation of social media content should only be done through accounts linked to a Unipol email address. Post to such sites must fully comply with GDPR.

Remote Access Viewing
Individual computers can be viewed remotely by senior management to ensure that computers are functioning but also to monitor abuse.

Unipol Board
A policy on visitors, observers, and other participants to board meetings has been agreed by the board

Any sensitive data collected from Board members for registration purposes (eg. Charity Commission) is destroyed once registration is complete.

Tenants' Photographs and Data Protection and Information Policy
Unipol collect photographs of tenants in certain developments provide proof of identity and to allow staff to more easily identify tenants captured on CCTV footage.

The following paragraph should be included in letter requesting the inclusion of a photograph:

"**GDPR**
Any information given by you or your institution regarding your tenancy, including photographs, 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. All personal information is dealt with according to Unipol's Data ProtectionPolicy. Copies are available on request."

Unipol Data Protection and Information Security Policy
Appendix 2:

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 and Information 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 Nikki Verity 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.

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;
- Information on people using our office wireless networks;
- Website usage and demographic information through Google Analytics;
- 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
Complaints	7 years	From submission
Payment transactions	7 years	From submission
Tenancy Agreement generator	3 months	From submission
Google Analytics tracking information	26 month	From submission
Firewall and server event logs	3 months	From submission

For more detail on how long we keep data retention for read our Data Protection and Information Policy.

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.

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, currently this option is only available to landlords.

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, responding STOP to any text messages 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 https://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.

Unipol Data Protection and Information Security Policy
Appendix 3: Request form for access to personal data

Unipol Student Homes
GDPR
You may find it helpful to Request access to personal data held by Unipol using this form.

I,

(Insert full name and your connection to Unipol ie owner, tenant)

wish to have access to

1. Either, data that Unipol has about me in one or more of the following categories:

(a)	data relating to applications for employment, staff review or career progression	□
(b)	employment or tenant – related references	□
(c)	any other statement of opinion about my abilities or perfomrance not included in (a) or (b) above	□
(d)	health and medical matters	□
(e)	disciplinary matters	□
(f)	data relating to a Code complaint	□
(g)	other information (please specify below)	□

_____

_____

_____

2. Or data that Unipol currently has about me , either as part of an automated system or part of a relevant filing system
□

I enclosemy proof of identity. Original documents are required.

Signed

Dated

Address for correspondance

Upon completion forward to:

Ms Nikki Verity
Company Secretary
Unipol Student Homes
155-157 Woodhouse Lane
Leeds
LS2 3ED
Telephone 0113 2430169

Unipol Data Protection and Information Security Policy
Appendix 4:

PCI DSS Cardholder Security Policy

Introduction
Unipol is responsible for keeping card account information safe and secure while being processing and transmitted irrespective of the nature of the transaction. Failure to do so could allow a fraud to be perpetrated; result in legal action being taken against us; fines being imposed by the service provider and our bank; reputational damage to Unipol and the withdrawal of card processing capabilities in the future.

The responsibilities for Information Security in relation to PCI DSS within Unipol lie with the Company Secretary.
To ensure ongoing compliance on an annual basis Unipol will:

- Review this policy in line with the Unipol Data Protection and Information Policy which will be submitted to the Board for approval before being circulated to staff
- Review PCI DSS requirements to identify any changes
- Review merchant services provider to ensure they are still verified to current PCI DSS standards and appoint new providers if required

Staff Access to systems
Access to devices capable of processing card payments will only be granted to authorised staff, who are trained annually in PCI DSS requirements, and will be secured by individual passwords. A list of user accounts along with a register of devices capable of processing card payments will also be centrally maintained.

Physically securing systems
To prevent tampering and substitution of POS hardware a centralised list of devices will be maintained which will record make, model, serial number and location of each item, this list will be audited at least twice a year and updated whenever any devices are changed or relocated. All devices will be fitted with tamper evident stickers which will be checked on a monthly basis to detect signs of tampering.

PED Merchant Receipts
All Merchant copy debit/credit card payment receipts are immediately secured in and transferred to the finance department; any which contain the customers primary account number (PAN) and the card expiration date are shredded within 3 days of the payment being taken and the funds having been received in Unipol bank account.

Staff responsibilities in processing card payments

- Do not handle customer cards or request PIN numbers.
- Do not electronically record / write down any card details on paper.
- Do not request card details via electronic or physical media, if this information is received unsolicited then they must be deleted / cross shredded and the sender informed not to re-send these details.
- Do not use card and verification details for any purpose other than completing the card transaction.

Direct Debits
Direct Debit information is taken electronically and via paper. All signed paper mandates will be retained in a secure manner in a locked cupboard/filing cabinet or securely held in electronic format in an user restricted filestore location. To increase protection of personal data Unipol are bringing on an electronic direct debit payment method. Online mandates are processed via a secure (HTTPS) connection and bank account information encrypted in an SQL database.

Electronic Payment Processing Requirements
A system called MOTO has been set up to enable appropriate staff to enter card holder details directly onto a computer screen in order to process payments.
Staff do not record or retain details in any format