

## **Unipol Data Protection and Information Security Policy**

### **September 2010**

#### **Main Policy**

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

*The code falls into two sections. The first, covered in paragraphs 1-48, constitutes a statement of general policy, which includes an indication of Unipol's obligations under the Act. The second section, covered in paragraphs 49-65, provides brief guidance notes for staff in connection with handling personal data.*

*There are three 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 Website Privacy Policy – to be put on the web site and linked from Unipol's front page, this informs Unipol's Website users how their data is dealt with; and Appendix 3: Request form for access to personal data*

#### **Introduction**

1. Unipol needs to process certain information about its employees, tenants, landlords and others. In so doing, Unipol must comply with the Data Protection Act 1998 [the Act]. The Act contains eight basic principles, which state that personal data must:

- be processed fairly and lawfully and only for the purpose(s) for which it was originally gathered
- data should not be obtained or processed unnecessarily
- be adequate, relevant and not excessive for those purposes
- be accurate and kept up to date
- not be kept for longer than is necessary for that purpose
- should be kept securely and not released to third parties without consent
- be kept safe from unauthorised access, accidental loss or destruction
- not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

2. Some of the notable features of the Act are 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 clients to personal data that relates to them* held in computerised systems and in 'organised' manual filing systems within the organisation.
- It places emphasis on data security, especially in relation to the unauthorised disclosure of personal data to third parties.

(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)

3. Unipol and all staff or others who process or use any personal information must ensure that the data protection principles and the law under the Act are 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 Metropolitan University's Code. The references to personal data made within this document apply to all data held on individuals within Unipol, not just clients.

#### **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 do so can result in disciplinary proceedings.

5. Any member of staff who considers that the policy has not been followed in respect of personal data should raise the matter with Unipol's designated data contact (the Deputy Chief Executive). If the matter is not resolved with the help of the data contact it should be raised under the relevant complaints procedures.

### **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 beliefs, trade union membership, health, sex life and criminal convictions. Under the Act the processing of sensitive data is subject to much stricter conditions.

9. The term processing covers almost anything that is done to data, namely, collection, use, storage and retention by reference to individuals.

10. Data subjects have the right of access to information held on them, through submission of a subject access request. There is no entitlement to immediate or on-site access to information. Unipol has a maximum of 40 days in which to comply with a request for access by a data subject. This is 40 ordinary days not working days.

### **Electronic data**

11. Electronically-held data encompasses not just personal data held on databases but, for example, emails, letters and other documents held on disk or on hard drive.

### **Manual filing systems**

12. 'Relevant' manual filing systems are covered by the Act. These may have the following characteristics:

- grouping within a common theme, even if not physically kept in the same file or drawer
- Structuring by reference to the individual by name, number or other mechanism, or by criteria common to individuals, such as sickness, type of job or property.
- and, most pertinently of all, *structuring that allows specific information about the individual to be readily accessible.*

13. In practical terms, however, it seems reasonable to assume that most, if not all, manual filing systems fall under the provisions of the Act.

### **Subject Consent**

14. 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.

15. 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. In such circumstances, Unipol will normally at the time of application advise applicants that they intend to seek such information and/or seek self disclosure.

16. All applicants for employment or prospective tenants are asked to signify their consent to Unipol processing both ordinary and sensitive personal data for the purposes of processing that application. Upon signing up for a property or acceptance of an offer of employment, tenants and staff are asked to give consent to processing a wider range of data. Agreement to Unipol processing these personal

data is a condition of acceptance of a tenant into any property and a condition of employment for staff; a refusal to provide consent may result in discontinuance of the application.

17. Consent to process the personal data of external inquirers or other users of Unipol's services will be unnecessary in most instances, 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**

18. 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 - partly in order to comply with statutory requirements but primarily as a way of maintaining a complete historical record.

### **Access to data**

19. Staff, tenants, landlords and other users of Unipol have the right to access any personal data that is being kept about them either on computer or in 'relevant' manual files. Any person who wishes to exercise this right should complete the access request form and forward it to the Deputy Chief Executive . Unipol will levy a charge of £10 on each occasion that access is requested.

20. 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 40 days from the date of the request unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the data subject making the request.

21. However, information about third parties must not be disclosed, unless they have given consent to disclosure. In the absence of consent, references to third parties should be deleted. Where this is not practical, access can be denied.

### **Staff responsibilities**

22. In addition to their responsibilities for processing personal data about tenants and landlords (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.*

23. In connection with their own personal data, all staff must:

- 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).

24. Any request for information by a third party should be referred to the Deputy Chief Executive.

### **Data Security**

25. All 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.

26. Staff should note that wilful unauthorised disclosure will usually be a disciplinary matter.

27. Staff must ensure that, where a data processor processes data on Unipol's behalf (a mailing agency, for example) there is a written contract 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.

28. 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 may need to be:

- kept in a locked filing cabinet, or
- in a locked drawer, or
- if it is computerised, be password protected, or
- kept only on disks which are themselves kept securely.

29. 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.

30. 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**

31. 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

32. 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**

33. It is regrettably the case that instances may arise of staff and clients using Unipol resources - including computers and telephones - to conduct unauthorised activities. Unipol must ensure that its resources are not used inappropriately or illegally; and may from time to time monitor staff communications without giving notice.

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.

34. For reasons of personal security and to protect Unipol premises and the property of tenants and staff, 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. This use is exempted from the Data Protection Act (Section 36 – Domestic Purposes Exception).

35. Tenants or staff who consider that their communications are being unfairly monitored or that the positioning of a closed circuit television camera is inappropriate should contact the designated data contact (see below).

### **World Wide Web and Email**

36. 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.
- 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 and abide by Unipol's privacy statement.

37. Unipol must ensure that its resources are not abused or used illegally. Unipol may from time to time monitor staff communications without giving notice. This is primarily to prevent the creation (including viewing) or transmission of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material (This could constitute an offence under The Malicious Communications Act 1988, The Obscene Publications Act 1959 & 1964, The Telecommunications Act 1984, and if children are involved, The Protection of Children Act 1978). Staff emails will also be read by a senior member of staff to ensure that essential correspondence is dealt with, for example when away or out of the office.

### **Cross-border data flows**

38. 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 ( or outside of areas that the EU considers to have adequate level of protection for personal data and US Companies complying with the 'Safe Harbour' scheme 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 (see also paragraph 36 above). The ICO website contains up to date information on which countries are considered to provide adequate levels of protection.

### **Research data**

39. 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.

40. 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.

41. 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 the Act.

### **Confidential references**

42. References remain confidential to the subject and the organisation. The subject may subsequently choose to see and/or distribute the reference to others. Where Unipol request a reference there is a clause making clear this policy.

43. 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.

44. 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.

### **The Unipol Code for Shared Student Housing, Unipol DASH Code for Shared Student Housing and ANUK/Unipol Code of Standards for Larger Residential Developments**

45. 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 ANUK/Unipol Code of Standards for Larger Residential Developments Codes are government approved schemes and as such data can be provided to Government (currently CLG) at their request.

### **Complaints**

46. 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 Deputy Chief Executive 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 Deputy Chief Executive. If the matter is not resolved with the help of the Deputy Chief Executive it should be raised with the Chief Executive.

### **Conclusion**

47. Compliance with the 1998 Act is the responsibility of all members of staff at Unipol. Any breach of the data protection 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 Assistant Chief Executive - Technical Services.

### **Further information**

48. 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 Deputy Chief Executive.
- 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](http://www.ico.gov.uk)

## GUIDANCE NOTES FOR STAFF

49. 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. 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.

50. 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 the Act.

51. 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.

52. 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.”

53. 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 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.

54. Senior Managers i.e. Chief Executive Deputy Chief Executive, Communications and IT Manager, Financial Controller, Development Manager, Assistant Chief Executive - Housing Services and Accommodation Bureau Manager Nottingham are the only staff authorised to hold or process sensitive data.

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

56. 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.

57. 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).

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

### Staff Checklist for Processing Data

59. 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**

60. 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 forty days in which to comply with data subject access requests - and *staff should forward all such requests to the Deputy Chief Executive.*

61. 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.

62. 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.

Only the Deputy Chief Executive or the Chief Executive are authorised to provide references on behalf of Unipol.

63. 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**

64. 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 Deputy Chief Executive. 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**

65. Further information and advice is available from the Deputy Chief Executive.

**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. 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 tenants details forms 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, the police and local government agencies) on request. 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 will also disclose the details of any Third Party, stated above in connection with your deposit, to the scheme administrators. We may also disclose your name and telephone number to a Unipol-approved contractor, in order that they may contact you to arrange to carry out a repair at your property.

If a Third Party (i.e. parent, carer, local authority, guarantor) is paying your rent directly to Unipol by 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 below. If you choose not to select a Third Party on this form, 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 to any Third Party.

**Unipol may discuss any issue relating to my Tenancy with:**

<b>Name</b>	<b>Daytime contact number</b>	<b>Relationship to Tenant</b>
-------------	-------------------------------	-------------------------------

**Unipol may discuss any issue relating to my rent account with:**

<b>Name</b>	<b>Daytime contact number</b>	<b>Relationship to Tenant</b>
-------------	-------------------------------	-------------------------------

**Leeds Met Allocated Tenants**

Leeds Met 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, 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 Metropolitan University to Unipol Student Homes, as part of the allocation procedure. (Leeds Met's full Data Protection Policy can be found on their website, [www.leedsmet.ac.uk](http://www.leedsmet.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 files**

- Finance staff keep records of all former tenants who are currently in debt and will also keep a record of who have paid back their debts within the last seven years and their retention dates.
- Files for these tenants will be kept separately with retained but nil debt former tenants being kept in 'to be destroyed' date order. These will be destroyed after seven years.
- The records will be used to ensure computer records are also destroyed in accordance with this procedure.

### **Retention of tenants files**

Tenants' correspondence files and supporting documentation including tenant details forms, correspondence files and agreements will be destroyed 7 years after the last correspondence with the tenant if the tenant no longer uses Unipol's services.

### **Sensitive data**

Data on tenants classified under the DPA 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.

### **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 Database

### **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 policy in relation to them on the Owners registration form.

Condition of Service states

"Data Protection Act 1998. 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."

**Unipol has a data sharing agreement with the Local Authority (the relevant name is inserted on the form) to share the information held in relation to student housing including (but not exclusively) property inspection information, landlords name and address, information regarding Code complaints and actions taken and details of Code members.**

#### **Owners files**

Registration forms and accommodation details forms are kept alphabetically in a lockable cupboard and are not accessible by the public.

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

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

#### **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."

#### **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.'

#### **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.

#### **Unipol Code for Shared Student Housing, Unipol DASH Code 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 Landlords Accreditation Scheme.

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 chair's 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 ANUK/Unipol Code of Standards for Larger Residential Developments Codes are government approved schemes and as such data can be provided to Government (currently CLG) 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.

### **Solicitor**

The Solicitor service is confidential between the solicitor and their clients. A client must give express permission for the solicitor to disclose information to the Code Officer or other appropriate member of Unipol staff. The solicitor will however provide statistics on the number of cases they have seen and a brief summary of the gist of the case and outcome to Unipol without identifying the client..

### **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.

Internet payments can be made for both the above.

### **Website privacy, Student Accommodation Discussion Group and Student to Student noticeboard**

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 Accommodation Bureau and 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.

Accommodation bureau house hunting enquiries sent by email will be kept for statistical purposes and deleted after 1 year. 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 1 year. Email with ongoing relevance can be kept and may be printed out and filed in the appropriate paper file.

Paper copies of emails and their retention time will follow the same guidelines as paper copies of other correspondence.

### **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. The Deputy Chief Executive will have overall responsibility for this area. The policy will be reviewed annually at the June meeting of the Sub Committee on IT Services..

### **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 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 Deputy Chief Executive..

### **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.
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 the Disability Discrimination Act.

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 or on the web.
19. Development of staff research profiles by associated University companies.
20. Monitoring the use of University and Unipol resources.
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 whom the Unipol 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.

(1). Sensitive personal data includes information relating to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life and criminal convictions.

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

#### **Guidelines for Retention of Personal Data**

<b>Type of Data</b>	<b>Maximum retention period</b>	<b>Reason for Length of Period</b>
Personnel files including training records and notes of disciplinary and grievance hearings	6 years from the end of employment	References and potential litigation
Application forms/interview notes	At least 8 months from the date of the interviews	Time limits on litigation
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 tax office	At least 3 years after the end of the financial year to which the records relate	Income Tax (Employment) Regulations 1993

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

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. Deputy Chief Executive, Communications and IT Manager, Financial Controller, Assistant Chief Executive - Housing Services, Development Manager, the Accommodation Bureau Manager Nottingham, the Supporte Officer to the Deputy Chief Executive 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 Chief Executive's directory or the Deputy Chief Executive's directory both of which have restricted access. This is only accessible by the Senior Managers i.e. Deputy Chief Executive, Communications and IT Manager, Financial Controller, Assistant Chief Executive - Housing Services, Development Manager and the Accommodation Bureau Manager Nottingham and the Support Officer to the Deputy Chief Executive. Where there are working documents on staff that are not in the Chief Executives directory they have the same restriction on access.

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 Chief Executive's directory.

#### **Staffing Matters** are reported to Unipol Board

The staffing sections of the agendas and minutes of the Financial Affairs and Staffing Sub Committee agendas are confidential to Board members and members of the Financial Affairs and Staffing Sub Committee. The staffing minutes from the Financial Affairs and Staffing Sub 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 shall be 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 within 8 months. If your application is successful and you are appointed, your information and future data will be processed in accordance with the Unipol Data Protection and Information Security Policy. A copy of this code can be obtained from the Unipol Website."

### **Staff References**

References given in confidence can remain in confidence. However it may be challenged that the receiver is under not confidence restrictions and so if Unipol receives it may have to be disclosed to the member of staff concerned.

References that Unipol gives do not have to be shared by the member of staff concerned however the receiver of the reference may choose to show it to the person.

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 the DPA Unipol 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 apart from a member of the Senior Management Team and the ICT Officer. No paper or computer notes of any passwords must be kept apart from those kept by the Communications and IT Manager 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.

### **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 Policy**

Unipol collect photographs from tenants in certain developments to allow staff to more easily identify tenants on CCTV footage.

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

#### **"Data Protection Act 1988**

Any information given by you 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 Protection and Information Security Policy. Copies are available on request."

## **Unipol Data Protection and Information Security Policy**

### **Appendix 2: Unipol Website Privacy Statement**

This explains how Unipol uses any information you give to us via our Website, and the ways in which we protect your privacy. It is not intended to be a privacy statement in relation to information submitted to Unipol by any other means.)

#### **The Data Protection Act 1998**

Unipol is a Data Controller under the Data Protection Act 1998. We hold information for the purposes of running the Unipol Accommodation Bureau, Unipol Housing, Unipol Training and certain other functions as agreed by the Unipol Board of Directors. Unipol complies with the data protection principles set out in the Data Protection Act 1998 in relation to personal data which you give to us via our Website to the extent that the Act requires it to do so. These principles restrict the powers of a data controller to disclose to third parties personal data which it is processing.

#### **What information do we collect via the Website?**

We collect four main types of information from online visitors to Unipol:

- Feedback (general questions and specific feedback on the Website);
- Booking and payment details from users of Unipol Training and those attending Unipol organised events;
- Payment details from property owners/agents, tenants and other users of Unipol;
- Site usage information (from session cookies and log files).
- Student to Student Noticeboard Messages
- Searches of the Accommodation Bureau database and personal clipboard lists

##### **1. Feedback, questions and comments**

You can send us your comments to our email feedback address or from our Website surveys that are presented from time to time. If you send an email or letter to us or call us for information, once we have replied to you, we keep a record of your messages for three months for reference and audit purposes, after which it may be deleted.

##### **2. Booking and payment details from users of Unipol Training**

Unipol Training uses on-line booking and payment facilities for its clients. This information is processed and kept on file. No information is disclosed to third parties without users consent. Records of credit card details are not stored on computer.

##### **3. Payment details from property owners/agents, tenants and other users of Unipol**

Unipol provides on-line payment facilities for its clients. No information is disclosed to third parties without users consent. Records of credit card details are not stored on computer.

##### **4. Student to Student Noticeboard Messages**

Messages entered onto the Student to Student Noticeboard are in the public domain. Messages are stored and have tracking information including the internet address of the computer used for entering the message stored as well. This can be used for tracking persistent abuse of the Noticeboard.

##### **5. Searches of the Accommodation Bureau database and personal clipboard lists**

Searches made and clipboards saved have tracking information including the internet address of the computer used for entering the message stored as well. This can be used for tracking persistent abuse of the site.

##### **6. Demographic Information**

[Unipol](#) collects aggregate information site-wide, including anonymous site statistics. On certain pages we give users the option of providing us with names, addresses, phone numbers, fax numbers, email addresses, demographic, preference and other personal information, and various other kinds of details. Such personal information is not gathered by us without users' knowledge, active permission and participation. We use contact data from our surveys to send the user information about our Website and company. The customer's contact information may also be used to contact the visitor when we believe it is necessary or appropriate. Users may opt-out of receiving future mailings; see the choice/opt-out section below. Information is also shared with advertisers on an aggregate basis.

## 7. Cookies

Portions of our site use "cookies" to keep track of your visit and to help you navigate between sections, thus delivering content specific to your interests and to give us an idea of which parts of our site users are visiting. A cookie is a small data file that certain Web sites write to your hard drive when you visit them. A cookie file can contain information such as a user ID that the site uses to track the pages you've visited. But the only personal information a cookie contains is information you supply yourself. A cookie does not read data from your hard disk or read cookie files created by other sites. This means that a user's session will be tracked, but the user will be anonymous.

Unipol displays advertising on the Website and we also use outside advertising companies to display advertisements on our site. These advertisements may contain cookies. While we use cookies in other parts of our Website, cookies received with banner advertisements are collected by our advertisers and/or advertising companies, and we do not have access to this information.

### **Security**

This site has 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, backup tapes, and conventional locks and alarm systems. However we cannot guarantee that the measures in place are (or will remain) adequate.

### **Choice/Opt-Out**

Our Website gives users the opportunity to opt-out of receiving communications from us at the point where we request information about the visitor. This site gives users the option to remove their information from our database, to not receive future communications or to no longer receive our service. You can edit your profile online or can send mail to the following postal address: Unipol Student Homes 155-157 Woodhouse Lane, Leeds LS2 3ED

Unipol may, from time to time, share your details with third parties who have products or services which may be of interest to you, such as universities and survey compilers. These third parties may in turn write or e-mail you with details of their products or services. If you did not opt out of this practice on our registration page, but do not wish your information to be used in this way, users are given the the option to change and modify information previously provided by them when they are logged in.

### **What happens when I link to another site?**

This website contains links to other Websites, both those of partner organisations and companies, government departments and of other organisations. This privacy policy applies only to our site, 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**  
**Data Protection Act 1998**

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 performance 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 understand that there is a fee of £10.00 payable to Unipol and this is enclosed, together with my Photo Driving license/passport/staff identity card/other (please specify) as proof of identity. Original documents are required.

Signed

Dated

Address for correspondence

Upon completion forward to:

Ms Liz Hodgen  
Deputy Chief Executive  
Unipol Student Homes  
155-157 Woodhouse Lane  
Leeds  
LS2 3ED  
Telephone 0113 2430169

## **Unipol Data Protection and Information Security Policy**

### ***Appendix 4: The Processing of Credit & Debit Card Payments & the Security of Cardholder Data Standard***

#### **Background**

Visa and MasterCard have jointly developed what is known as the Payment Card Industry Data Security Standard (PCI-DSS) to minimise the risk of fraud from misuse of card details and other customer payment information. The Standard applies to all merchants (of which Unipol is one) who store, process or otherwise have access to cardholder information. The Standard, which is endorsed by American Express, JCB and Diners Card, details the measures that are to be taken to ensure that the cardholder data is secure.

Organisations that record, process and retain payment card data in electronic format have to be Certified against the Standard, whereas those who take credit and debit card payments by other means have to comply with the Standard. Chip and PIN (Personal Identification Number) payments, where the cardholder is present, are outside the scope of PCI-DSS.

It is not appropriate for Unipol to become Certified and instead Unipol outsourced the collection of electronic card payments to Certified third parties who process the data on Unipol's behalf. However a review of current business practices has been carried out to ensure that we fully comply with the Standard in all other areas.

#### **Our Responsibility**

Unipol is responsible for keeping card account information safe and secure whatever the method of storage, processing or transmission, and 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; large fines being imposed by the card schemes and our bank; reputation damage to Unipol and the withdrawal of card processing capabilities in the future.

#### **Processing Payments by Credit/ Debit Cards Requirements**

- Do not record credit and debit card details on paper.
- Do not use card and verification details for any purpose other than completing the card transaction.
- Do not pass this information to anyone else, except for the purpose of helping you to complete the card transaction.
- Once processed do not store the card security code (the last 3 digits on the card signature strip provided when the card holder is not present)) under any circumstances.
- Do not keep a separate record of the card number and expiry date:

#### **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.**

Deputy Chief Executive.