The University of Chichester

Data Protection Policy

1. Introduction

1.1 The Data Protection Act 1998 ("the Act") gives rights to individuals, including staff and students, about whom information or "personal data" is obtained or processed. This Policy does not distinguish between manual and electronic processing of data.

1.2 This Policy summarises and explains the legal obligations placed upon the University of Chichester (the "University") with regard to its data processing activities.

1.3 The University is fully committed to complying with its obligations under the Act, in respect of all processing of personal data in connection with its business and in so doing meeting the expectations of its staff and students.

1.4 A "data subject" is any individual about whom the University processes personal and/or sensitive personal data.

1.5 "Staff", "students" and "other data subjects" may include past, present and potential members of those groups. "Other data subjects" and "third parties" may include contractors, suppliers, contacts, referees, friends, family members, or any other person that the University conducts its business with.

2. What is Personal Data?

2.1 Personal data is information which relates to a living individual (ie not companies) who can be identified from that information, (whether directly or indirectly on its own or in conjunction with any other information held).

2.2 Personal data must relate to that individual's personal, private, business or professional life. Examples of personal data that the University may process from time to time in its day to day business are detailed in Appendix 1.

3. What is processing?

3.1 Data processing is the collective term for any action or operation carried out in relation to personal data. This includes collection, use, transfer, download, amendment, storage, deletion and retention of personal data by the University, amongst other tasks.

3.2 The purposes for which personal data is processed by the University are set out in Appendix 2 to this Policy. If the University processes personal data for new or amended purposes, it will update this Policy to notify staff, students and other data subjects accordingly.

3.3 As a result, the University recommends that staff, students and other data subjects check this Policy regularly to ensure that they are aware of the latest version and any relevant changes from time to time.

4. Sensitive Personal Data

4.1 Sensitive personal data is personal data relating to:

Policy approved by the Board of Governors – 25 November 2008
Policy & Appendices reviewed and updated: December 2017

- race;
- political opinions;
- health (physical or mental);
- religious beliefs;
- trade union membership;
- criminal records and alleged offences;
- racial or ethnic origin;
- sexual life.

4.2 The University may, in some circumstances, be obliged by law to process sensitive personal data about a data subject. For example, some jobs or courses will bring the applicants into contact with children, including young people between the ages of 16 and 18, and the University has a duty under the Children Act 1989 and other enactments to ensure that staff are suitable for the job, and students for the courses offered by making certain criminal checks. The University may also require such information for the administration of the sick pay policy, the absence policy or the equal opportunities policy, or for academic assessment.

4.3 There are additional legal requirements placed upon the University where it is processing sensitive personal data. In some cases the University requires the explicit consent of the data subject before processing any of his/her data. Students may provide their consent at the time of acceptance of a course; staff may provide their consent at the time of employment by signing an explicit notice of consent.

4.4 The University also asks for information about particular health needs, such as allergies to particular forms of medication, or conditions such as asthma or diabetes. The University will only use such information where legally permitted to do so, to protect the health and safety of the individual, for example, in the event of a medical emergency.

4.5 In certain limited circumstances, the University does not have to obtain an individual's consent to process his or her sensitive personal data. The circumstances most relevant to the University are:

- the processing is necessary to protect the vital interests of the data subject (where consent cannot be given by the data subject or cannot reasonably be obtained by the University) or of another person (where consent by the data subject has been unreasonably withheld - for example in a medical emergency).
- the processing relates to information deliberately made public by the data subject;
- the processing is necessary for an employment related legal (not contractual) obligation;
- the processing is carried out by a health professional and is necessary for medical purposes; or

- the data relates to racial or ethnic origin and is processed in the context of equal opportunity monitoring.

5. The Rules for Processing Personal Data

Any personal data shall be processed in accordance with the eight Data Protection Principles contained in the Act. These are that personal and sensitive personal data must:

1) be processed fairly and lawfully;
2) be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with the purpose;
3) be adequate, relevant and not excessive for the purpose;
4) be accurate and up-to-date;
5) not be kept for longer than necessary for the purpose;
6) be processed in accordance with the data subject's rights;
7) be kept safe from unauthorised processing, and accidental loss, damage or destruction; and
8) not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data, except in specified circumstances.

In addition, the University cannot use or process Personal Data unless one or more conditions are met. The conditions most relevant to the University are:

- the data subject has given consent to the processing;

- where necessary to enter a contract with a data subject at their request or to perform a contract with a data subject; or

- where a legitimate business interest is proportionate (i.e. not unwarranted having regard to the rights and freedoms or legitimate interests of the data subject)

This overlaps with the University's legal obligations under human rights legislation.

6. Rights of Access to Information

6.1 The University has a central procedure for dealing with all requests for access to personal information, in accordance with the provisions of the Act. A data subject may ask for their own Personal data (a "subject access request"). The Act does not generally permit a person to see Personal Data about other people. Generally, if such a valid subject access request is made the University will (if requested):

- advise the data subject whether it is processing any personal data concerning them (or on their behalf);

- if so, give the data subject a description of that personal data, the purposes for which the data is being processed and the recipient or classes of recipient to whom it is or may be disclosed by the University;

- tell the data subject, in an intelligible and permanent format (unless the cost of such permanent format would be disproportionate), the information contained in that personal data and its source; and

- if relevant, advise the data subject of the logic involved where a decision relating to or significantly affecting the data subject is made on the basis of processing that personal data by automatic means.

6.2 All requests will be dealt with by the Data Protection Officer within 40 days of receipt of the valid request from the individual in writing (unless there is good reason for delay, in which case, this reason will be explained in writing by the Data Protection Officer to the data subject making the request). For a valid request the applicant must clearly identify themselves and their request for their Personal Data and pay a £10.00 access fee made payable to the University of Chichester. Any requests received by staff must be passed immediately to the Data Protection Officer. The University may defer dealing with a subject access request while it requests (and until it receives) proof of identity of an applicant and/or the £10 fee.

6.3 Staff, students and other data subjects have the right to access personal data that is being processed about them. Any person may exercise this right by submitting a request in writing to the Data Protection Officer in accordance with 6.2 above.

7. Further Data Subject Rights

7.1 In addition to the right of access, every data subject has a right to require that the University corrects or deletes any inaccurate data held about him/her. Any requests for inaccuracies to be corrected should be addressed to the University's Data Protection Officer. The University is not obliged to do so in all cases. In that situation the University will normally note the comments of the data subject in relation to the relevant data.

7.2 If the data subject believes that the University is going to process his or her data in a way that would be damaging or distressing to him or her, (s)he has the right to object to the University processing his/her personal data in that manner. In such circumstances the University will review the data processing which is the subject of the complaint and will stop data processing where required under the Act. It may not have to (or be legally able to) stop all data processing.

7.3 The data subject is entitled, by written notice, to require the University to ensure that no decision which significantly affects that data subject is based solely on the processing by automatic means of the data subject's personal data.

7.4 Any data subject has the right to request the Commissioner to assess whether any provision of the Act has been contravened by the University. This is a serious step which should not be abused and which should not be taken as a last option if matters cannot be reasonably agreed with the University.

8. Data Accuracy

8.1 Personal data must be kept accurate and where necessary up to date. It must be adequate, relevant and not excessive for the purpose it was collected for.

8.2 The University will take reasonable steps to ensure accuracy and quality of personal data, and to prevent it becoming out of date. Staff members and students will receive regular requests to update their personal data and are responsible for doing so promptly and accurately. Staff and students must provide the University with true and accurate data and promptly notify it, where relevant, of any changes to it. Any incorrect or out of date data will be removed as soon as possible.

9. Data Security

9.1 Personal data will be stored and managed securely in compliance with this Policy and the University of Chichester Electronic Information Security Policy.

9.2 Personal data must be kept and handled securely (both for electronic and paper records) and all staff must take precautions against physical loss or damage occurring to personal data and to minimise unauthorised access. Staff, students and other relevant data subjects must ensure that both access to and disclosure of their personal data is restricted as appropriate. The University expects staff to be responsible for ensuring that appropriate security measures are taken. For example:

- computers are locked at all times when unattended;
- a sensible password on computers, laptops, tablets and mobile phones is set;
- memory sticks should not be used to store sensitive personal information, and in any case should be encrypted
- passwords are not shared or left unsecured and are changed when required; and
- Sensitive material is treated carefully, stored separately and not left unattended.

9.3 Sensitive personal data must be protected with a higher level of security. It is recommended that sensitive records are kept separately in a locked drawer or filing cabinet, or in a password-protected computer file. Where such information is required to be accessed from outside of the University's campuses, this should be by storing it in a network drive location, using the remote access tools provided and this should be with the prior written authority of their supervisor and in accordance with any conditions set. The measures taken to safeguard such information should be implemented in accordance with the Policy referred to at para 9.1 above. If a member of staff, or a student, is holding, or intending to hold, sensitive personal information which is outside standard University processing, e.g. for a research project, the Data Protection Officer should be notified with details as soon as possible.

10. Retention of Data

The University will keep different types of information for different lengths of time, depending on legal, academic, fiscal and operational requirements. The retention periods of the data that the University processes is detailed in Appendix 3.

11. The Data Controller and the Designated Data Controllers

The University is the data controller under the Act, and the Vice-Chancellor is ultimately responsible for its implementation. The Data Protection Officer will be responsible for dealing with daily issues.

12. Assessment Marks

Students shall be entitled to information about their marks for assessments; however this may take longer to provide than other information. The University may withhold enrolment, awards, certificates, accreditation or references until monies or any other financial obligations due to the University have been paid.

13. Compliance

13.1 Compliance with the Act is the responsibility of all students and members of staff. Any deliberate or reckless breach of this Policy or action which leads to the University being in breach of its obligations under the Act may lead to disciplinary, and where appropriate, legal proceedings.

13.2 Any individual, who considers that the Policy has not been followed in respect of personal data about him or herself, should raise the matter with the Data Protection Officer initially. If the matter is not resolved it should be referred to the staff grievance or student complaints procedure.

14. Staff Responsibilities

All staff shall comply with the "Data Protection Guidelines for University Staff" (Appendix 4).

15. Student Responsibilities

All students shall comply with the "Student Data Protection Statement" (Appendix 5).

16. Computer Equipment

Students and staff must comply with the University's policies, in particular the University of Chichester Electronic Information Security Policy and the Code of Conduct for the use of IT facilities and/or email systems.

17. Other Use

17.1 The University receives public funding and accordingly is subject to audit as a matter of law and to comply with the requirements of funding agreements. Such audits may involve processing personal data but are carried out subject to strict legal and/or contractual controls.

17.2 The University is sometimes, unfortunately, involved in claims and/or investigations. Personal Data may be processed, where necessary, in relation to crime prevention, national security and/or dealing with legal proceedings or taking legal advice.

17.3 The University necessarily works with many partners to operate successfully and in doing so must sometimes be subject to strict contractual controls, disclose or share Personal Data with such partners or service providers. In some cases, these partners are in other countries whose laws do not protect personal data or data subject rights as well as our laws. In those cases, it is still possible to send personal data to that country if you are satisfied that in the particular circumstances personal data and rights are protected by other means to adequately safeguard them, as required by law. Any queries should be referred to the Data Protection Officer.

Appendix 1

University Information Processing

The University has notified the Information Commissioner that personal information may need to be processed for the following purposes:

- Staff, Agent and Contractor Administration
- Advertising, Marketing, Public Relations, General Advice Services
- Accounts & Records
- Education
- Student and Staff Support Services
- Research
- Other Commercial Services
- Publication of the university magazine
- Graduation and alumni relations
- Police/solicitors
- Prevention and detection of crime

Complete details of the University's current entry on the Data Protection Register can be found on the notification section of the Information Commissioner's web site. Select the option to **Search Register** and when the search form is displayed, type University of Chichester into the Name box and then click on **Search.**

The register entry provides:

- a fuller explanation of the purposes for which personal information may be used (in broad but not detailed terms)
- details of the types of data subjects about whom personal information may be held
- details of the types of personal information that may be processed
- details of the individuals and organisations that may be recipients of personal information collected by the University
- information about transfers of personal information.

Appendix 2

Data Protection Guidelines for University Staff

---

1. **Introduction**
The revised Data Protection Act 1998, which is concerned with the handling of personal information, came fully into force on 1 March 2000. This Act is more stringent than the 1984 Act as, among other things, it covers both manual and electronic records and stipulates security standards. All staff share responsibility for processing data in accordance with the Data Protection Act.

2. **Standard Information**
Most staff process information about students on a regular basis e.g. taking registers, writing reports or references, data input to the University's central student information database (SITS), or as part of a pastoral or academic supervisory role. The University will ensure through registration procedures that all students are notified of such processing, as required by the Act, and give their consent where necessary. The information that staff deal with on a day-to-day basis is "standard" and covers categories such as:

- General personal details such as name, address and date of birth;
- Details about class attendance, course work marks and grades and associated comments;
- Notes of personal supervision, including matters about behaviour and discipline;
- Sponsorship details.

3**.** **Sensitive Information**
Information about a student's physical or mental health, ethnicity or race, political or religious views, trade union membership, sexual life, or criminal record is sensitive information under the Act. Such information can only be collected and processed as required by law, e.g. by the Children Act 1989, or with the student's **express (written) consent**. Examples:

- Disability records
- keeping of sick notes;
- recording information about dietary needs, for religious or health reasons, prior to taking students on a field trip;
- recording information that a student is pregnant, as part of pastoral duties.

Disclosure of such information without consent is permitted only in "life or death" circumstances, e.g., if a student is unconscious, a tutor can tell medical staff that the student is pregnant or a Jehovah's Witness.

Sensitive information must be protected with a **higher level of security**. It is recommended that sensitive records are kept separately in a locked drawer or filing cabinet, on an encrypted device or password-protected computer file. Where such information is required to be accessed from outside of the University's campuses, this should be by storing it in a network drive location and by using the remote access tools provided. The measures taken to safeguard such information should be implemented in accordance with the University of Chichester Electronic Information Security Policy. If you (or one of your students) are holding, or intending to hold, sensitive personal

information which is outside standard University processing, e.g. for a research project, you should notify the Data Protection Officer.

4. **Processing of Personal Information**

Processing refers to any action involving personal information, including obtaining, viewing, copying, amending, adding, deleting, extracting, storing, disclosing or destroying information. When processing personal information, you must comply with the **data protection principles**, which are set out in the Data Protection Policy. In particular, you should ensure that records are:

- Accurate;
- up-to-date; and
- fairly and legally obtained.

University data should not be made available to unauthorised persons, or for unauthorised activity. University data should never be stored on personal computers which are accessed by private individuals. Personal computers which use wireless connections should always use secure connections.

Emails and any electronic attachments that contain personal information must remain on University systems and not be sent or received on staff's personal (non-work) email accounts. Staff in this context includes any authorised person who has been provided with a system logon account.

5. **Exemption for Research Records**

There is an exemption under the Data Protection Act 1998 for research and statistics. Information collected for the purpose of one piece of research can be used for other research, without breaching the "specified processing" principle (see the Data Protection Policy), and can be kept indefinitely. For example, staff and students involved in academic research can keep records of questionnaires and contacts, so that the research can be re-visited at a later date, or so that, in support of a research project looking at an associated area, they can re-analyse the information. Researchers must ensure that the final results of the research do not identify the individual, or they will be subject to access requests under the 1998 Act.

This exemption is only applicable to academic research, i.e. the personal data are not processed to support measures or decisions relating to particular individuals; and are not processed in such a way that substantial damage or distress may be caused to the data subject(s), e.g. following research carried out for a redundancy or efficiency exercise.

6. **Research**

If you supervise students doing work which involves the processing of personal information, you should ensure that those students are aware of the Data Protection Principles and the University Ethics Policy. Students should be referred to the Data Protection Officer for further information.

Notwithstanding the exemptions referred to above, most of the data principles still apply to research which uses personal data, notably the requirement to keep data secure and for specific measures to be taken on each occasion data are collected for research purposes.

If the data are completely and genuinely anonymised and no "key" to the identity of the data subject is held by (or is likely to come into the possession of) a researcher, then

the Data Protection Act does not apply, as such information is not considered to be "personal data" within the terms of the Act (i.e. data which relate to a living individual who can be identified from those data). However, if identification is at all possible, the Act still applies.

Generally, those collecting personal data as part of a research project must inform research subjects, as far as possible, and from the outset:

- the purpose of the research for which personal data about them will be collected;
- how their personal data will be used; and
- who will have access to their data.

It is expected that research applications will include an explanation and/or demonstration of how these measures will be taken.

It should also be noted that a research subject has the right to object to the processing of data on the grounds that such processing would cause them (or has caused them) significant damage or distress.

7. **Handling Enquiries**

When students ask to see information about themselves, you should, where possible, deal with these enquiries informally. If an informal response is not appropriate, you should advise the student to make a formal **Subject Access Request** under the Data Protection Act. Such Requests should be directed to the Data Protection Officer.

You should not disclose personal information over the **telephone** unless you are able to validate the identity of the student.

You may disclose personal information to **other staff members** who require the information in order to carry out their normal duties.

You should not disclose personal information to any **third party**, e.g., to a parent or sponsor, except with the consent of the student.

In **exceptional and urgent circumstances** (e.g., cases where there are reasonable grounds for believing that an individual has become a danger to him/herself or others, or has committed / is about to commit a serious crime), you may release personal information directly to a law officer. Please contact the Data Protection Officer in such cases. Be sure to establish the identity of the law officer before releasing the information, and get an emailed or faxed copy of the request, and keep a record of the incident including name, date, circumstances and information disclosed.

8. **Examination Marks**

You should be aware that students are now entitled to see preliminary marks and comments, which contribute to final assessments. Committee minutes will also be subject to access requests unless they are anonymised.

Similarly, when writing an **academic reference**, you should keep in mind that it may be subject to an access request by the student to the recipient.

9. **Private Files**

The case for holding "private", separate files has to be justified as being in the interest of the student (e.g., where the data is particularly sensitive) and the information contained in them will be subject to the student's right of access. To ensure

compliance with the notification requirements of the Act, you must inform the Data Protection Officer that you are holding such files. Wherever possible, you should avoid duplication or fragmentation of student files.

10. **Remote Access**

When working remotely on a University laptop, you should use the remote access services to store private and confidential information on the University's network drives. It is recommended that you do not work on USB memory sticks, or store any data on the laptop itself, as these can be lost and stolen. Private and Confidential University information should not be stored on any device not owned by the University, and even when using a University laptop:

- Special care should be taken in the transport of confidential information (particularly that which is personal information relating to people other than yourself).
- If it is absolutely necessary to do so, only ever carry paper files, laptops and memory sticks in a locked briefcase.
- If it is absolutely necessary to leave brief cases containing papers, laptops or memory sticks unattended, please store them in a locked office or locked away in your home.
- Never leave briefcases and laptops in your car.
- If it is absolutely necessary to use them, memory sticks must be encrypted and these should not in any case be used to store or transit confidential information.
- Emails that contain personal information must remain on University systems and must not be sent or received on staff's personal (non-work) email accounts.

For full information, please refer to the University's Electronic Information Security Policy: http://www.chi.ac.uk/about-us/how-we-work/policies/it-and-information-policies

Appendix 3

STUDENT DATA PROTECTION STATEMENT

This Statement explains how the personal data, including sensitive personal data, the University of Chichester collects from you may be used, which includes all aspects of the academic administration of your study, associated financial matters such as fees and bursaries, your personal welfare, and your access to University facilities.

The University has a central procedure for dealing with all requests for access to personal information, in accordance with UK data protection legislation. As a data subject you are entitled to ask for your own Personal data (a "subject access request"). Data protection legislation does not generally permit a person to see Personal Data about other people. For enquiries: email dpofficer@chi.ac.uk.

We use student data for internal reporting and statistical analysis connected with the management and planning of the University, and for compliance with legal obligations such as monitoring of Equality of Opportunity.

Whilst student data is mostly collected and maintained through the Academic Registry, the University will disclose that data to authorised users within the University to support the activities described above. The Academic Registry uses a student tracking system (SITS:Vision) and the bulk of processing within this system is undertaken under contract with you via the student registration and re-registration processes. All processing activities will take place in accordance with applicable legislation.

Our policy is to disclose information outside the University only if you have asked us to do so, or have agreed to the release of data, or if we are under a contractual or legal obligation to release the data. We may, for example transfer personal data to UCAS to enable them to provide retention and other student support as part of its duty of pastoral care but in these circumstances only anonymised data will be returned to the University for the purposes of assisting us to improve our student retention strategies.

The list below includes some of the uses to which the University will put your personal data, however, it is not possible to list all of the uses to which the University will put your personal data, nor to list all of the bodies with whom we might have to share your personal data, where we have a legitimate reason in connection with your time here at the University to use that data, or where the University is under a legal requirement to provide data.

We shall not disclose information about you to third parties, even to a parent or guardian, without your explicit consent, other than in specific circumstances, see paras 17,18 and 19 below.

1. STATUTORY RETURNS

We are required by the Higher Education Funding Council for England (HEFCE) to collect certain data which is passed to the Higher Education Statistics Agency (HESA). HESA also require us to contact graduates and ask about their employment after leaving the University.

2. TEACHER EDUCATION STUDENTS

For students on courses of Initial Teacher Training, we are required to report to the National College for Teaching and Learning (NCTL) so that certificates of Qualified Teacher Status can be issued by them. We will also pass to NCTL the University of Chichester email

addresses of QTS students to enable NCTL to contact students direct regarding their QTS certificate.

3. INTERNAL AND EXTERNAL SURVEYS

HEFCE also requires us to pass contact information about finalists to Ipsos MORI to carry out the National Student Survey (NSS). HESA's Fair Collection Notices can be seen on the HESA website: https://www.hesa.ac.uk/about/regulation/data-protection/notices and more information about the NSS on the NSS website: http://www.thestudentsurvey.com.

We may provide your name and University email address for the Nationwide HE Survey as part of Active Universities Sport England Themed funding round, which aims to tackle gaps in sporting participation.

We participate in several national surveys of student experience and engagement, e.g. the Postgraduate Taught Experience Survey, where your student email, address and certain demographic information such as age are linked to your responses. To participate in these surveys respondents must read and check the data protection statement, which will be included, before commencing the survey, allowing data to be used in this way.

4. SLC AND LOCAL AUTHORITIES

Other examples where we are under an obligation to disclose data are the provision of information to the Student Loans Company or to Local Authorities in connection with Council Tax or the Electoral Register (although if in relation to the latter, students will be offered an opt-out). Our Tuition Fee Policy states that we may disclose information to a Debt Collection Agency appointed by us should you fail to pay fees due to the University.

5. TURNITIN

The University requires all students to submit their assessed coursework assignments via Turnitin. You should be aware that in submitting work to Turnitin for text matching, or as part of an e-submission pilot, you are agreeing with Turnitin®UK that it can be electronically checked for matches with existing sources and that an Originality Report can be generated.

The final submission you make to any Turnitin assignment will be kept on the Turnitin®UK database *permanently.* Work held on the Turnitin®UK database may be used for the purpose of detecting the future plagiarism of your own work and or in any investigation of suspected academic malpractice.

Originality Reports - generated by you or a member of staff - may be used to assist in the identification of plagiarised work submitted for formal assessment. An Originality Report will never be advanced as the sole reason for suspecting that a piece of work is plagiarised, nor may an Originality Report be advanced as the sole defence against an accusation of plagiarism.

Turnitin®UK has a Privacy Pledge and a Usage Policy. It is recommended that you familiarise yourself with the contents of these.

6. HOME OFFICE: UK Visas & Immigration (UKVI)

Should you be from outside the EU, we are required to disclose information relating to your registration, attendance and progression to the UKVI.

7. PLACEMENTS

If you are on a course of study at the University which requires study, employment or a placement at another organisation it may be necessary for the University to transfer personal data to that organisation. Personal or sensitive personal data, however, will not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data, other than in specified circumstances.

8. STUDENT ATTENDANCE

The University has implemented an attendance management system, which operates by recording students tapping in to on-campus timetabled sessions. The primary purpose of this system is to enable relevant staff to more quickly identify students who, based on their non-attendance, may be at risk of under-achieving, being deregistered, or leaving the University entirely. Students will be able to see their own attendance records for their on-campus, timetabled sessions. Communications about any absences will be stored in the attendance management system, and will only be accessible by the student and relevant staff members. Attendance data will be stored securely on on-site servers and transferred to Microsoft Azure Cloud Server until the student graduates, after which time data will be fully anonymised and only used for historic trend analysis.

9. THE HEAR

Since academic year 2013/14, as part of a national initiative an electronic Higher Education Achievement Report (HEAR) (incorporating the European Diploma Supplement) is produced for Foundation Degree and Undergraduate Degree students on programmes based at the BOC and BRC campuses. Students will receive this in addition to their degree certificate.

The HEAR adheres to a national template and provides a broader range of information than the existing academic transcript/European Diploma Supplement. The document will be owned by the University and all information included, will be formally verified.

The HEAR will be delivered via a secure web portal called Gradintel. This cloud service will receive and hold personal data about you from our Student Records System and will be delivered and supported by the suppliers (Tribal) of the University's admissions and student records system. Students will receive full instructions about how to activate their accounts via Gradintel so that they can access information released at any time during their time at University and afterwards. Students will have access to their HEAR in perpetuity via Gradintel. More information about the HEAR can be found here:
http://www.chi.ac.uk/study-us/student-services/welcome-careers-and-employability-service/hear

10. REFERENCES AND CONFIRMATION OF QUALIFICATIONS

The University may release data about you in response to a request for a reference or for confirmation of your qualifications. Please note that we will only comply with a reference request where it is clear that the enquirer has the right to ask for the information, which will typically involve the consent of the former student to disclose their information. Further information about how third parties can verify qualifications can be found here:
http://www.chi.ac.uk/study-us/student-services/welcome-careers-and-employability-service/services-relating-former

11. UNIVERSITY OF CHICHESTER STUDENTS' UNION

The University shares student personal data with the University of Chichester Students' Union (UCSU) in order for the Union to administer membership of the UCSU and its clubs and societies, to communicate with members, to hold elections of officers, to ensure the safety and security of members (including identification of individual members) to provide welfare services, to market services provided directly by the UCSU and to analyse service provision and membership requirements. This may include passing personal data to a third party organisation which provides website and membership systems for Universities and Students' Unions. In such circumstances, however, student personal data will remain the property of the University and will not be used by the third party organisation for commercial or marketing purposes, or passed to any other third party. In all other circumstances the information provided to the SU shall not be passed to any third party, without your express consent. The UCSU shall implement appropriate mechanisms for students to opt out of membership of the Students' Union and to opt out of the use by the UCSU of all or any of their data at any time.

In addition to the above, personal data may be shared between the University and UCSU where this is in connection with an emergency, serious health or welfare issue or in relation to the prevention or detection of crime.

This data sharing is in accordance with a Data Sharing Agreement between the University and UCSU, which is located here: http://www.chi.ac.uk/about-us/how-we-work/policies/data-protection

12. STUDENT PHOTOGRAPHS

We store the photograph used on your student Campus Card but we will not display your photograph publicly (e.g. on notice-boards) without consent or release your photograph outside the University.

The University may occasionally commission photographs around the campuses or at specific events such as Graduation and those may include images of students for inclusion in promotional material.

13. ALUMNI RELATIONS

Graduating students will automatically become members of The Alumni Association unless you choose to opt out. Finalists will be contacted before Graduation and you will be able to 'opt out' of having your name or award used in commemorative publicity material or added to the Alumni database. You may withdraw from these communications at any time by contacting alumni@chi.ac.uk.

14. CCTV

We use CCTV in some areas where students' images may be routinely captured and stored for a limited period, solely for prevention of crime and apprehension and prosecution of offenders.

15. DISABILITY

We ask you about any disability you may have to enable us to support you should you have a disability. You can refuse to tell us about a disability but we will then not be able to support you so easily. We monitor the numbers of students with a disability, and the type of disability, to support our legal obligations in relation to Equality of Opportunity.

16. EQUAL OPPORTUNITIES MONITORING

We will ask you about your ethnicity and we use that data only for the purposes of EO monitoring. You can refuse to tell us about your ethnicity.

17. LAW ENFORCEMENT AGENCIES

We disclose information to law enforcement agencies (such as the Police) only where they invoke their statutory powers in connection with the prevention or detection of crime, and then only when we are satisfied that the request has been properly made.

18. EMERGENCIES

The Data Protection Act allows us to release data about you or about the person named by you for contact in emergency e.g. to a hospital or medical professional when your health is at risk and you are not able to give your specific consent. Our Student Services staff will always keep any record maintained to support your health and wellbeing confidential, and staff will explain any specific Confidentiality Policies.

19. HEALTH INFORMATION

Information on a student's health may be required prior to admission to certain programmes of study and for purposes linked with academic progress and examinations. Information about a student's health may also be necessary when a student undertakes fieldwork e.g. for health and safety or insurance purposes. The University may, in exceptional circumstances, contact third parties such as medical professionals or next of kin regarding the health of a student when it believes this to be reasonable and/or in the best interests of the student concerned. In these circumstances the University will attempt to gain the prior consent of the student but where consent cannot or will not be given it may act without consent.

The University will also use your contact details to keep you informed of initiatives relating to your time at the University e.g. careers services or postgraduate studies, as well as to provide details of the Alumni Association. If you do not wish to receive these communications please contact the University's Data Protection Officer – contact details are given at the end of this Statement.

You can request a copy of the data we hold about you, although you are able to see and update most of that data yourself via the Student Portal. The University's Commitment Charter sets out our pledge:

> Safeguard information you supply in compliance with the requirements of the Data Protection Act, the Freedom of Information Act or any other statutory obligations of the University; to explain to you why we need to collect information.

We will retain your full student record for five years after you have left the University so that we can fulfil our function of recording details of the awards we make and provide details of your education and references when asked to do so. After these five years we will retain transcript data in order to confirm details of your award.

In return ALL students shall:

- ensure that all personal information which they provide to the University is accurate and up-to-date;

- inform the University of any changes to that information, for example, changes of address;

- check the information which the University shall make available from time to time, in written or electronic form, and inform the University of any errors or, where appropriate, follow procedures for up-dating entries on computer forms. The University shall not be held responsible for errors about which it has not been informed.

Students who use the University's computer facilities may, from time to time, process personal information (for example, in course work or research). In all such circumstances the processing of personal data must comply with the requirements of the Data Protection Act. Students must seek guidance from the Faculty accordingly. The Faculty may also wish to refer the student to the Data Protection Officer.

Where can I get advice/further information?

More information is available on the Data Protection pages of the web or via the on-line Student Handbook. For enquiries: email dpofficer@chi.ac.uk

Appendix 4

Details of personal data processed by the University including Retention Periods

The following information is held in separate documents:

Part 1 University of Chichester: corporate systems involving the processing of personal data

Part 2 University of Chichester: all other personal data processing activities

For further information contact the University Data Protection Officer dpofficer@chi.ac.uk