University of Nottingham Students' Union

Staff Privacy Notice (May 2018)

The University of Nottingham Students' Union is committed to protecting and respecting your privacy. This policy sets out the basis on which any personal data we collect in the course of your employment will be processed by us. Please read this privacy notice carefully to understand your rights and our views and practices regarding your personal data.

For the purpose of data protection legislation, the controller is The University of Nottingham Students' Union, Portland Building, University Park, Nottingham, NG7 2RD.

This policy is overseen by the Data Protection Manager ("**DPM**"). If you have any requests or complaints please contact the DPM at OS-SUDataProtection@Nottingham.ac.uk.

What information do we collect from you?

We will collect and process the following data about you:

- **Information you give us.** This is information about you that you give us directly. You may do this by filling in forms or by corresponding with us by phone, email or otherwise. Information may be provided by you in meetings and appraisals. Additionally, information you enter onto our systems and devices will be stored and processed by us. This will include any emails or other electronic messages and any documents, photos or other files stored on or processed through our systems or devices. Please be aware that by entering information onto these systems you are sharing that information with us.
- **Information we collect throughout our relationship.** We will collect information throughout your time with us. This may include information about location, access to systems, outputs, working hours, absences, and other information relating to the performance of your role.
- **The type of information we collect.** This may include, but is not limited to the following:
    - **Identification information** - name, date and place of birth, gender, photograph, biometrics, ethnic origin, marital status, nationality and government identification numbers, student number and course details (if applicable);
    - **Contact details** - address, telephone/email address, emergency contact details;

- **Employment related information** - job title, work contact information, CV and employment application, eligibility to work, employment history, references, qualifications and other educational history, employment contract information, pension plan participation information, benefits information, performance record, appraisals, disciplinary record and absence record, relationship status with any Students' Union employees, details of criminal convictions, health records & physician details ;
- **Financial information** - bank account details, tax information, salary, benefits, expenses, company allowances, third party remuneration sources;
- **Spouse and dependent information** - next of kin and family contact details;
- **IT related information** - information collected by your use of our information systems and other computer equipment (such as email).
- **Equality and Diversity** – You may choose to share information about your health, ethnicity, sexuality or beliefs with us for equality and diversity purposes. This information will be treated as highly confidential.
- **Other data** which we may notify you of from time to time.

- **Information we receive from other sources.** We receive information about you from third parties, including:
  - Tax and regulatory authorities such as HMRC;
  - Previous employers;
  - Recruitment or vetting agencies;
  - Other employees and workers;
  - Business contacts;
  - Publicly available resources including online sources;

Why do we collect this information?

We use this information in the following ways:

- **Information you give to us and that we collect.** We process your Personal Data for the following reasons:
  - **Pursuant to your employment contract** in order to:

- conduct payroll, expenses, compensation, bonus and tax administration (as applicable);
- conduct personnel administration, including administration of any employee benefits;
- monitor performance, appraisals, absences, disciplinaries, grievances and other investigations; and
- review ongoing health issues and records including occupational health reports and self-certification forms.

- On the basis of your **consent or explicit consent** for the purpose of:
  - Supporting you to make a claim on the income protection insurance (where applicable)
  - Where we rely on your consent for processing this will be brought to your attention when the information is collected from you.

- In our **legitimate interest** for the purpose of:
  - informing you about work-related events and opportunities, both during your employment and afterwards;
  - hiring and recruitment and the processing of job applications including any employment background checks, reference checks and qualifications and training checks;
  - monitoring and enforcing compliance with our policies and procedures and applicable law to ensure a compliant workplace;
  - promotion and salary progression exercises
  - allowing access to and monitoring of our IT and security infrastructure including the use of CCTV footage in our offices and on our sites;
  - carrying out and reviewing employee surveys and communicating with you generally in our legitimate interest for improving our business and workplace;
  - production of published staff lists including telephone and email directories for both internal and external use;
  - production of staff badges and identity cards;
  - providing and obtaining references and consultation with external agencies;
  - promotion and salary progression exercises;

- training and development;
- for our legitimate interest in respect of litigation, including bringing or defending legal claims; and
- accounting and financial planning purposes.

You have the right to object to processing carried out for our legitimate interests. See the **What are your rights?** section below for more information.

- To comply with **legal requirements** relating to:
  - data protection;
  - tax;
  - health and safety;
  - anti-money laundering;
  - anti-discrimination;
  - mandatory reporting obligations;
  - disclosures required by law enforcement agencies;
  - fraud investigations; and
  - any other legal obligations placed on us from time to time.

- **Information we receive from other sources.** See the 'Who might we share your information with?' section below for details of how we use information in conjunction with third parties.
- **Photographs.** You may be included in images taken in the course of business. Uses may include use in promotional materials, social media or newsletters, use on an online profile, for identification purposes on passes and online systems, on wall displays to identify you as a fire warden, first aider or a similar role, or for similar business purposes.

We may inform you of additional purposes for processing your information when that information is collected from you.

How long do we keep hold of your information?

We only store your information for as long as is required for the purpose it was collected. For much of your information, this will be for the length of your employment with us and then for a period of 6 years thereafter.

We will retain some information relating to your training and working conditions for long term health and safety reasons such as to defend against claims of injury or disability.

Information stored generally on IT systems, such as email history, will be deleted regularly in line with our policies.

Please see the table below for more examples of data retention periods:

Type of data	**Retention policy**
Personnel files including training records, notes of disciplinary/grievance meetings etc.	6 years from the end of employment
Application forms/interview notes etc.	6 months from the date of the interviews
Facts relating to redundancies where less than 20 redundancies	3 years from the date of redundancy
Facts relating to redundancies where more than 20 redundancies	12 years from date of redundancies
Wages and salary records	7 years
Accident books, and records and reports of accidents	3 years after the date of the last entry
Records kept by reason of the Control of Substances Hazardous to Health (COSHH) regulations 2002	40 years
Records kept by reason of the Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR) regulations 2013	40 years

Who might we share your information with?

Where information is shared with third parties we will only share the information required for the purpose it is being shared.

For the purposes set out in the 'Why do we collect this information?' section above, we have the right to share your personal information with:

- Our sub-processors and service providers including training providers, pension providers, other workplace benefits providers as notified to you from time to time, occupational health providers, IT service providers,

HMRC, payroll provider, and legal advice provider. Details of which can be provided upon request.

Additionally, we will disclose your personal information to the relevant third party:

- In the course of business, to other organisations and individuals as required in relation to your role and duties.
- In the event that we sell or buy any business or assets, in which case we will disclose your Personal Data to the prospective seller or buyer of such business or assets.
- To third parties when it is necessary for the establishment, exercise or defence of legal claims.
- If we are acquired by a third party, in which case Personal Data held by it about its customers will be one of the transferred assets.
- If we choose to exercise a legal power to do so.
- If we are under a duty to disclose or share your Personal Data in order to comply with any legal obligation, or in order to enforce or apply contractual terms or other agreements; or to protect the rights, property, or safety of ourselves our customers, our regulator, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and prevention of money laundering and credit risk reduction.

How is your data stored and kept secure?

At the University of Nottingham Students' Union, we take your safety and security very seriously and we are committed to protecting your personal and financial information. All information kept by us is stored on secure servers. Where we have given you (or where you have chosen) a password that enables you to access certain systems, you are responsible for keeping this password confidential and changing it when prompted to do so. We ask you not to share a password with anyone; doing so could put personal and business data at risk and could lead to disciplinary action.

Once we have received your information, we will use strict procedures and security features to try to prevent unauthorised access. We operates a Data Protection and Information Security Policy for our employees and volunteers. All employees and volunteers handling data are required to undertake general data protection training. Personal data is password protected and/or secured in dedicated systems to hold the data with access being restricted to only those individuals within the Union who need access. Paper copies containing person data will be kept in a locked filing cabinet and

shredded/destroyed at the end of the appropriate retention period **OR** scanned in and immediately shredded/destroyed.

We may transfer your data outside the European Economic Area ("EEA"). We will only do so if adequate protection measures are in place in compliance with data protection legislation. We use the following protection measures:

- transferring to Commission approved countries;
- using Commission approved model contractual clauses;
- requiring companies we transfer data to in US to be signed up to the appropriate certification e.g. Privacy Shield.

Once we have received your information, we will use strict procedures and security features to try and prevent unauthorised access. More information is available by contacting us.

What are your rights?

You have the following rights. You can exercise these rights at any time by contacting us at University of Nottingham Students' Union, Portland Building, University Park, Nottingham, NG7 2RD OR OS-SUDataProtection@Nottingham.ac.uk. You have the right:

- to ask us not to process your personal data where it is processed on the basis of legitimate interests provided that there are no compelling reasons for that processing;
- where processing of your personal data is based on consent, to withdraw that consent at any time.
- to request from us access to personal information held about you;
- to ask for the information we hold about you to be rectified if it is inaccurate or incomplete;
- to ask for data to be erased provided that the personal data is no longer necessary for the purposes for which it was collected, you withdraw consent (if the legal basis for processing is consent), you exercise your right to object, set out below, and there are no overriding legitimate ground for processing, the data is unlawfully processed, the data needs to be erased to comply with a legal obligation;
- to ask for the processing of that information to be restricted if the accuracy of that data is contested, the processing is unlawful, the personal data is no longer necessary for the purposes for which it was collected or you exercise your right to object (pending verification of whether there are legitimate grounds for processing);

- to ask for data portability if the processing is carried out by automated means and the legal basis for processing is consent or contract.

Should you have any issues, concerns or problems in relation to your data, or wish to notify us of data which is inaccurate, please let us know by contacting us using the contact details above. In the event that you are not satisfied with our processing of your personal data, you have the right to lodge a complaint with the relevant supervisory authority, which is the Information Commissioner's Office (ICO) in the UK, at any time. The ICO's contact details are available here: https://ico.org.uk/concerns/.

What we ask of you

- **Keeping your information accurate and up to date.** If your information changes for any reason, for example if you change your name, address or bank, then you should inform us of the change as soon as possible so that we can ensure your information is kept accurate and up to date. If you are unsure who to notify then ask your line manager.

- **Personal data that you provide about another person.** If you provide us with information about another person, for example, about your dependents, next of kin or emergency contacts, you confirm that you have informed them of our identity, the purposes for which their personal data will be processed (e.g. for emergency contacts or benefits purposes) and that you have obtained their permission to such processing.

- **Business cards.** If you are issued with business cards as part of your role, your data will be processed by those who you share the business cards with. It is reasonably expected that the data will only be processed by those you share it with for business purposes, principally, to contact you in relation to your role and to the role or business of those you share the cards with.

Definitions

Personal Data: Any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier, such identifiers including name, identification number, location data or online identifier.

Special Categories of Data includes data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Changes to our privacy policy

This policy may be updated from time to time. You will be notified of any changes to this privacy notice.

Contact us

Questions, comments and requests regarding this privacy policy are welcomed and should be addressed to your line manager in the first instance. If you still have queries or concerns or if you are not comfortable discussing with your line manager then you can contact the DPM at OS-SUDataProtection@Nottingham.ac.uk.