NUS
Data Protection Policy

Policy Name:	**Data Protection Policy**	**Policy No:**	HR034
Approval Date:	December 2020	**To Be Reviewed:**	Annually
Approved By:	NUS HR Subcommittee		
Noted / Endorsed:	NUS UK Director and NUS Charity Director *TUNE*		
Document Location:	*G:\HR SHARE\HR Policies*		
Related Policies / Procedures:	Information Technology Privacy Statements All HR Policies		

REVIEW HISTORY

Date	Version Number	Name	Signature	Notes
October 2016	V1	Jayne Beer		*New Policy*
September 2017	V2	Jayne Beer		*Updated re new DPO / GDPR review date*
March 2018	V3	Sharon Pass		*Updated to reflect GDPR changes*
Sept 2019	V4	Jane Gilchrist		*Review and Amendments*
Nov 2020	V5	Jane Gilchrist		*Review and minor amendments*

Data Protection Policy Statement

NUS is committed to all aspects of data protection and takes seriously its duties, and the duties of its employees, under the General Data Protection Regulation (GDPR). This policy sets out how the organisation deals with personal data, including personnel files and data, subject access requests, and employees' obligations in relation to personal data.

Contact: The HR Team
e: hrteam@nus.org.uk

1. Purpose

1.1 All organisations create and maintain data during the course of business. This policy sets out the organisation's commitment to data protection. The policy aims to ensure that all colleagues are aware of the requirements of data protection legislation in relation to their individual rights as well as their individual obligations.

2. Scope

2.1 The policy applies to all employees of National Union of Students (UK), NUS Students' Union Charitable Services and NUS Holdings Ltd, unless they are expressly excluded. The policy applies to full or part-time employees. The policy also applies to agency workers, volunteers and self-employed contractors in relation to their assignments or volunteering at NUS.

2.2 The policy also applies to the processing of personal data of job applicants and contractors as well as the personal data of clients or other personal data processed for business purposes.

2.3 Where the policy refers to 'NUS' it means both National Union of Students (UK) and NUS Students' Union Charitable Services or a company under their control. At time of writing these are: NUS Services Ltd [controlled by NUS Students' Union Charitable Services] and NUS Holdings Ltd [controlled by National Union of Students (UK)].

2.4 This policy does not form part of an employee's contract of employment and it may be amended at any time. Amendments to this policy will be discussed, and if necessary agreed, with the recognised trade union as identified in the union recognition agreement.

2.5 The organisation has a Data Protection contact- Davina Keen, Membership Director. Their role is to inform and advise the organisation on its data protection obligations. They can be contacted at dpo@nus.org.uk. Questions about this policy, or requests for further information, should be directed to the Data Protection contact. If they are not available (or where issues need to be further escalated) issues should be referred to the relevant Director.

3. Legislation

3.1 The General Data Protection Regulation (GDPR) applies in the UK from 25 May 2018 and is the legislation governing data protection in the EU. This piece of legislation has significantly changed data protection law in the UK.

3.2 The GDPR will apply directly in the UK before its departure from the EU. When the UK leaves the EU, the GDPR will be incorporated into UK law by the European Union (Withdrawal) Bill. The Government has also published the Data Protection Bill, which will supplement GDPR standards in the UK. The Bill will replace the Data Protection Act 1998.

3.3 The GDPR controls how personal information is used by organisations, businesses or the government. Everyone responsible for using data has to follow strict rules called '**data protection principles'**, (see section 5).

4. Definitions

4.1 '**Personal data**' means any information relating to an identified or identifiable natural person ('**data subject'**); an identifiable natural person is one who can be identified,

directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

4.2 **'Processing'** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

4.3 '**Special categories of personal data'** means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

4.4 '**Criminal records data'** means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

4.5 A data subject is an individual who is the subject of personal data i.e. the individual whom particular personal data is about. The legislation does not count as a data subject an individual who has died or who cannot be identified or distinguished from others.

4.6 Organisations that initially collect personal data are '**data controllers'** and individuals to whom the data relates are '**data subjects'**. For example, the terms data controller and data subject would refer to employers and employees respectively.

4.7 A data controller is a person or organisation who determines the purposes for which and the manner in which any personal data, are, or are to be, processed. This means that the data controller exercises overall control over the 'why' and the 'how' of a data processing activity. The data controller will be legally responsible for ensuring that the processing complies with the legislation, including the collection, storage, use, alteration, disclosure and destruction of information.

4.8 A '**data processor**' is any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Example - If working with another organisation this would be a colleague in the other organisation handling the data as part of the project. For example, NUS is sometimes the data processors for our member unions who use UnionCloud, where we decide to look at trends in voter turnout at a national level.

4.9 '**Consent'** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to them.

4.10 '**Personal data breach'** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

5. Principles

5.1 NUS is obliged to abide by the data protection principles embodied in the legislation. The data protection principles that anyone responsible for using data must abide by are as follows:

- Personal data shall be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('**lawfulness, fairness and transparency'**);

- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘**data minimisation’**);

- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘**accuracy**’);

- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (**‘storage limitation’**);

- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘**integrity and confidentiality’**)**.**

- The ‘accountability’ principle means that NUS is required to demonstrate compliance with the above principles through e.g. staff training, internal audits of processing activities, reviews of internal HR policies, maintaining relevant documentation on processing activities and so on.

5.2 The organisation is committed to being transparent about how it collects and uses the personal data of its workforce, and to meeting its data protection obligations.

5.3 All employees are under an obligation to ensure that they have regard to the data protection principles when accessing, using or disposing of personal information. Failure to observe the data protection principles within this policy may result in an employee incurring personal criminal liability. It may also result in disciplinary action up to and including dismissal. For example, if an employee accesses another employee's employment records without the requisite authority, the organisation will treat this as gross misconduct and instigate its disciplinary procedures. Such gross misconduct will also constitute a criminal offence.

5.4 The organisation informs individuals of the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons.

5.5 Where the organisation processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with NUS’ privacy notice regarding special categories of data and criminal records data.

5.6 The organisation will update HR-related personal data promptly if an individual advises that their information has changed or is inaccurate.

5.7 Personal data gathered during the employment, worker, contractor or volunteer relationship, or apprenticeship is held in electronic format. This may be in individual employee files, on HR systems or other electronic databases. The periods for which the organisation holds HR-related personal data are detailed in the data retention schedule (appendix 1).

5.8 The organisation keeps a record of its processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

6. Impact assessments

6.1 Some of the processing that the organisation carries out may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, the organisation will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

7. Personal data

7.1 The GDPR applies only to information that constitutes '**personal data'**. Information is personal data if it:

- identifies a person, whether by itself, or together with other information in the organisation's possession, or is likely to come into its possession; and

- is about a living person and affects that person's privacy (whether in their personal or family life, business or professional capacity) in the sense that the information has the person as its focus or is otherwise biographical in nature.

- Consequently, automated and computerised personal information about employees are covered by the Regulations. Personal information stored physically (for example, on paper) and held in any '**relevant filing system**' is also covered. In addition, information recorded with the intention that it will be stored in a relevant filing system or held on computer is covered. In the employment context, this will include information in an employee's personnel file, information held on HR systems, information contained in emails and information obtained through employee monitoring.

- A '**filing system**' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

8. The processing of personal information

8.1 The GDPR applies to personal information that is '**processed**'.

8.2 '**Processing**', in relation to information or data means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including—

- organisation, adaptation or alteration of the information or data,
- retrieval, consultation or use of the information or data,
- disclosure of the information or data by transmission, dissemination or otherwise making available.

8.3 An individual's duties under the GDPR apply throughout the period when processing personal data – as do the rights of data subjects. Employees must comply with the regulations from the moment they obtain the data until the time when the data has been returned, deleted or destroyed.

8.4 An individual's duties also extend to the way they dispose of personal data when the data is no longer needed. The data must be disposed of securely and in a way which does not prejudice the interests of the individuals concerned.

9. When personal information can be processed

9.1 Data processing should only take place where:

- it is necessary for the completion of a contract with the data subject; or
- the organisation has a legitimate interest in processing data; or
- it is necessary to protect the interest of the individual or carry out public functions; or
- there is a legal obligation to process the information or
- where the person who the information is about has given permission; knows who is using the information; knows what they are using it for; and knows who it is likely to be passed on to.

9.2 The rationale for processing different types of data is set out in the relevant privacy notice.

10. Special Categories of personal data

10.1 As defined above, '**special categories of personal data**' means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.

10.2 The presumption is that, because information about these matters could be used in a discriminatory way, and is likely to be of a private nature, it needs to be treated with greater care than other personal data.

10.3 NUS retains special categories of personal data for the purposes of statistical monitoring or in line legal obligations as outlined in employment contracts and privacy notices.

10.4 NUS will process sensitive personal data, including sickness and injury records and references, in accordance with the data protection principles.

11. Employee responsibilities in relation to personal data

11.1 Individuals are responsible for helping the organisation keep their personal data up to date. Individuals should let the organisation know if data provided to the organisation changes, for example if an individual moves house or changes their bank details.

11.2 Individuals may have access to the personal data of other individuals and of our customers and clients in the course of their employment, contract, volunteer period or apprenticeship. Where this is the case, the organisation relies on individuals to help meet its data protection obligations to staff and to customers and clients.

11.3 Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);

- not to remove personal data, or devices containing or that can be used to access personal data, from the organisation's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to store personal data on local drives or on personal devices that are used for work purposes.

11.4 Further details about the organisation's security procedures can be found in its IT policy and are documented in the privacy notice.

11.5 Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under NUS' Disciplinary Policy. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

11.6 In order to strengthen the enforcement of the rules of GDPR, penalties including personal fines may be imposed by the Information Commissioner's Office (ICO) for infringement of the Regulations.

11.7 In a case of a minor infringement or if the fine likely to be imposed would constitute a disproportionate burden to an individual, a reprimand may be issued instead of a fine. Due regard would be given to e.g. the nature, gravity and duration of the infringement, the intentional character of the infringement, actions taken to mitigate the damage suffered, degree of responsibility or any relevant previous infringements, compliance with measures ordered against the controller or processor, any other aggravating or mitigating factors.

11.8 NUS provides compliance training on data protection issues to all employees during induction (via e-learning). The organisation will continue to provide such employees with refresher training at regular intervals thereafter. Separate induction arrangements are made for agency workers, contractors and volunteers.

11.9 Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, are required to sign additional confidentiality agreements to ensure compliance with this policy.

11.10 Certain employees – who have access to special categories of personal data – are also required to sign separate confidentiality agreements as part of their contract of employment.

11.11 If an employee acquires any personal information in error by whatever means, they shall inform the Data Protection contact immediately and, if it is not necessary for them to retain that information, arrange for it to be handled by the appropriate individual within the organisation.

11.12 If an employee is in any doubt about what they may or may not do with personal information, they should seek advice from the Data Protection contact. If they cannot get in touch with the Data Protection Contract, they should not disclose the information concerned.

11.13 All software packages within NUS are password protected. Where individuals are given a password in order to deliver their activities, they may not share this password with other colleagues. When an individual is given a password, they will be entered onto a register of users for that software held centrally in the IT department. The IT department will change the password every 90 days and also if someone on the register leaves or starts with the organisation.

12. Manager Responsibilities

12.1 Managers must ensure that employees are made aware of this policy and the responsibilities contained therein.

12.2 Managers must also ensure that employees complete the mandatory GDPR training available on Workrite

12.3 Where managers or a member of their team needs to purchase a software package which retains '**personal data**', as defined within the legislation, they must liaise with the IT department prior to acquisition of that software. IT will be able to advise on data protection, software licensing and IT compliance requirements.

12.4 Managers must ensure that they inform IT of all applications used by their team so that IT can manage passwords/accounts appropriately on a schedule, including when staff leave/start with the organisation. No software should be purchased without first speaking with IT.

13. Personnel files

13.1 An employee's personnel file is likely to contain information about their work history with the organisation and may, for example, include information about any disciplinary or grievance procedures, warnings, absence records, appraisal or performance information and personal information about the employee including address details and national insurance number.

13.2 There may also be other information about the employee located within the organisation, for example in their manager's inbox or in files; with payroll; or within documents stored in a relevant filing system.

13.3 The organisation may collect relevant sensitive personal information from employees for diversity monitoring purposes. Where such information is collected, the organisation will anonymise it unless the purpose to which the information is put requires the full use of the individual's personal information. If the information is to be used, the organisation will inform employees on any monitoring questionnaire of the use to which the data will be put, the individuals or posts within the organisation who will have access to that information and the security measures that the organisation will put in place to ensure that there is no unauthorised access to it.

13.4 The organisation will ensure that personal information about an employee, including information in personnel files, is securely retained. Information stored electronically will be subject to access controls. Passwords and encryption software will be used where it is necessary to share this data with third parties (e.g. pension providers).

14. Individual Rights

14.1 As a data subject, individuals have a number of rights in relation to their personal data.

15.Right of Access

15.1 Individuals have the right to access information kept about them by the organisation.

15.2 If an individual makes a subject access request, NUS will tell them:

- whether or not their data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;

- to whom their data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long their personal data is stored (or how that period is decided);
- their rights to rectification or erasure of data, or to restrict or object to processing;
- their right to complain to the Information Commissioner if they think the organisation has failed to comply with their data protection rights; and
- whether or not the organisation carries out automated decision-making and the logic involved in any such decision-making.

15.3 NUS will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless they agree otherwise.

15.4 If the individual wants additional copies, NUS will charge a fee, which will be based on the administrative cost to the organisation of providing the additional copies.

15.5 To make a subject access request, the individual should send the request to dpo@nus.org.uk. In some cases, NUS may need to ask for proof of identification before the request can be processed. The organisation will inform the individual if it needs to verify their identity and the documents it requires.

15.6 NUS will normally respond to a request within a period of one month from the date it is received. In some cases, such as where NUS processes large amounts of the individual's data, it may respond within three months of the date the request is received. NUS will write to the individual within one month of receiving the original request to tell them if this is the case.

15.7 If a subject access request is manifestly unfounded or excessive, NUS is not obliged to comply with it. Alternatively, NUS can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the organisation has already responded. If an individual submits a request that is unfounded or excessive, the organisation will notify them that this is the case and whether or not it will respond to it.

16.Other rights

16.1 Individuals have a number of other rights in relation to their personal data. They can require the organisation to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override the organisation's legitimate grounds for processing data (where the organisation relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the organisation's legitimate grounds for processing data.

16.2 To ask the organisation to take any of the steps in 16.1, the individual should send the request to hrteam@nus.org.uk.

17. Correction, updating and deletion of data

17.1 If an employee becomes aware that the organisation holds any inaccurate, irrelevant or out-of-date information about them, they must notify The HR Team immediately and provide any necessary corrections and/or updates to the information.

18. Data that is likely to cause substantial damage or distress

18.1 If an employee believes that the processing of personal information about them is causing, or is likely to cause, substantial and unwarranted damage or distress to them or another person, they may notify the organisation in writing to the Data Protection contact to request the organisation to put a stop to the processing of that information.

18.2 Within 21 days of receiving the employee's objection to processing, the organisation will reply to the employee stating either:

- that it has complied with or intends to comply with the request and how; or
- the reasons why it regards the employee's notice as unjustified to any extent and the extent, if any, to which it has already complied or intends to comply with the notice.

19.Data Protection Breaches

19.1 Any breach of personal data that poses a risk to the rights and freedoms of individuals must be reported to the Data Protection contact and the Data Protection Breach Response Evaluation Form (included as Appendix 2) must be completed in order to assess the nature of the problem and ascertain any future preventative action that should be put in place to avoid a repeat of the situation.

19.2 It will be the Data Protection contacts responsibility to report breaches to the Information Commissioner's Office (ICO) within 72 hours of discovery, unless the controller is able to demonstrate, in accordance with the accountability principle that the personal data breach is unlikely to result in a risk to the rights and freedoms of individuals. Where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay.

19.3 The organisation will record all data breaches regardless of their effect.

19.4 If the breach is likely to result in a high risk to the rights and freedoms of individuals, the Data Protection contact will inform affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

20.International data transfers

20.1 The organisation will not transfer employee-related personal data to countries outside the EEA.

21. Monitoring

21.1 NUS may monitor employees by various means including, but not limited to, recording employees' activities on CCTV, checking emails, listening to voicemails and monitoring telephone conversations. If this is the case, the organisation will inform the employee that monitoring is taking place, how data is being collected, how the data will be securely processed and the purpose for which the data will be used. The employee will usually be entitled to be given any data that has been collected about them. The organisation will not retain such data for any longer than is absolutely necessary.

21.2 In exceptional circumstances, the organisation may use monitoring covertly. This may be appropriate where there is, or could potentially be, damage caused to the organisation by the activity being monitored and where the information cannot be

obtained effectively by any non-intrusive means (for example, where an employee is suspected of stealing property belonging to the organisation). Covert monitoring will take place only with the approval of the DATA PROTECTION CONTACT.

Appendix 1.

Data Retention Schedule

Employees and Former Employees

Category of Data	Stored	Records Held	Retention Period / Deletion Approach
Records provided during recruitment, new starter processes and created during the course of employment	Electronic HR Employee Correspondence files Workrite	New Starter info. Performance Management records. Additional Needs declarations. Occupational Health & DSE Records. Risk Assessments and Personal Emergency Evacuation Plans (PEEPs). Mandatory Training data. First Aiders & Fire Marshalls. DBS information (result of check only).	Duration of employment See below for former employees
Absence during Pregnancy and Statutory Maternity Pay	Moorepay/SelectPay Electronic HR Employee Correspondence files	Payslips Payroll notes Moorepay record MATB1 form	Three years after the end of the tax year in which the employee's maternity pay period ended. Records reviewed on an annual basis (at the end of each tax year) and deleted
Statutory Paternity Pay, Statutory Shared Parental Leave Pay, Statutory Adoption Pay	Moorepay/SelectPay Electronic HR Employee Correspondence files	Payslips Payroll notes Moorepay record MATB1 form	Three years after the end of the tax year in which payments of SPP, ShPP or SAP were made. Records reviewed on an annual basis (at the end of each tax year) and deleted
PAYE records that employers are not otherwise required to send to HM Revenue and Customs under the Income Tax (Pay As You Earn) Regulations 2003.	Moorepay/ SelectPay	Payroll records: including name; address; payslips (or other record showing gross earnings, tax, national insurance contributions and student loan deductions, and net pay); Records used to complete P11Ds	Three years after the end of the income tax year to which the records relate. Records reviewed on an annual basis (at the end of each tax year) and deleted

Category of Data	**Stored**	**Records Held**	**Retention Period / Deletion Approach**
Right to Work	Electronic HR Employee Correspondence files	Records of documents sufficient to establish that the worker has the right to work in the UK, evidenced by a number of specified documents (or two documents in specified combination) from List A or List B as set out in the Immigration, Asylum and Nationality Act 2006.	For the period of employment and two years post-employment. For former employees Records reviewed on a monthly basis and deleted once two-year post-employment milestone reached.
Contracts of Employment	Electronic HR Employee Correspondence files	Contracts retained to ensure hold accurate records of role title and pay obligations.	Duration of employment and for seven years after employment ends. For former employees Records reviewed on an annual basis (at the end of each tax year) and deleted
Grievance & Disciplinary Documents	Electronic HR Employee Correspondence files	Investigation reports, interview statements, relevant background information, letters associated with formal processes	For 18 months after grievance outcome delivered or disciplinary outcome confirmed. See below for former employees.
Leave Records (Holiday, Sickness, Jury service etc.)	Moorepay Electronic HR Employee Correspondence files	Moorepay/SelectPay records (where leave has pay impact) e.g. unpaid parental leave.	Duration of employment. See below for former employees.
Equal Opportunities monitoring information, Dependants details. Next of Kin	Moorepay Electronic HR Employee Correspondence files	Information provided during recruitment and new starter process – either via Applicant Tracking System (ATS) or electronic form (next of kin etc.)	Duration of employment. Information is held as Employee Self Service and employees can check and update at any time. See below for former employees.

Category of Data	Stored	Records Held	Retention Period / Deletion Approach
Pension records	Moorepay/Shared with Aegon or Royal London Electronic HR Employee Correspondence files	Information provided during recruitment and new starter process – via electronic form. Information provided during auto-enrolment process or initiated by employee wishing to join pension scheme. Completed opt out forms if an employee wishes to leave the pension scheme.	Duration of employment. See below for former employees.
Accident Reporting	Accident book and Moorepay records (from October 2019 onwards)	Name, Home address and occupation of person affected. Name, home address and occupation of person reporting the incident if not the injured person. Date of accident/incident.	Records kept for 3 years then destroyed.
Driving Licence, Car Insurance and MOT status	Electronic Facilities Team files	Driving licence number, type, endorsements (if any) and validity dates. Car insurance document, car registration number and model details along with validity dates of MOT.	For current employees records kept for 3 years then destroyed. For former employees records kept for 12 months after leaving then destroyed.
Membership Card System for building entry and CCTV (Belfast office)	Information held by Ormeau Baths (Shared office provider) and Nest security provider	Card - Staff name only Security video – CCTV in plain sight, sound and images recorded.	Card data - deleted on leaving employment CCTV Recordings deleted after 2 weeks.
Swipe Card System for building entry (Macclesfield and Edinburgh office locations)	Information held on Server in Macclesfield	Staff name and office location only.	Records reviewed and staff leavers deleted on a quarterly basis.

Former Employees

Documents for leavers (where noted above as different from current employees) will be retained as follows:

Category of Data	**Stored**	**Records Held**	**Retention Period / Deletion Approach**
Records provided during recruitment, new starter processes and created during the course of employment which are held on file at the leaving date	Moorepay Electronic HR Employee Correspondence files	New Starter Documentation Performance Management documentation Equal Opportunities Monitoring information. Additional Needs declarations Occupational Health Records. Grievance and Disciplinary Records. Risk Assessments and Personal Emergency Evacuation Plans (PEEPs). Leave records	12 months after leaving date. HR Records reviewed and deleted on a monthly basis once 12-month post-employment milestone reached. People Managers advised to delete performance management documentation on an annual basis.
Pension Records	Electronic HR Employee Correspondence files	Information provided during recruitment and new starter process – via electronic form. Information provided during auto-enrolment process or initiated by employee wishing to join pension scheme. Completed opt out forms if an employee wishes to leave the pension scheme.	6 years after leaving date
Mandatory Training	Workrite Electronic HR Employee Correspondence files	Mandatory Training records.	12 months after leaving date. Records reviewed and deleted on a quarterly basis once 12-month post-employment milestone reached.
Health & Safety – First Aiders	Health & Safety Electronic files	Staff name and office location only	12 months after leaving date.

and Fire Marshal Training			Records reviewed and deleted on a quarterly basis once 12-month post-employment milestone reached.
Individual files, folders and email accounts	One drive Outlook	Emails sent / received and saved in folders, inbox and sent mail Files and folders created on individual one drive	12 months after leaving date for all employees in Bands A – H. Two years after leaving date for all employees in Bands I – L. Leavers encouraged to review documents retained prior to leaving employment and ensure transfer to shared folders / deletion as appropriate. Records reviewed and deleted on a monthly basis once relevant post-employment milestone reached.
Driving Licence, Car Insurance and MOT status	Electronic Facilities Team files	Driving licence number, type, endorsements (if any) and validity dates. Car insurance document, car registration number and model details along with validity dates of MOT.	For former employees records kept for 12 months after leaving date then destroyed.

Appendix 2.

Data Protection Breach Response Evaluation Form

Questions	Answers
Name	
Job Title	
Date	

Who is the executive director ultimately responsible for the area of work where the breach has taken place?	
Which NUS teams are affected by the breach?	
What is the data?	
How many people are affected?	
Where is the data now and how many people have seen it?	
What is being done to recover the data?	
How did the data loss occur?	
What policies are in place?	
What training/ awareness raising measures have been taken in the light of this episode?	
When did this episode begin?	
Has this happened before?	

Completed forms should be submitted to the Data Protection contact at dpo@nus.org.uk