|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **[System name] System User Access Form** | | | | | | |
|  | | | | | | |
| **Section 1 – to be completed by the person requesting access** | | | | | | |
|  | | | | | | |
| **Forename:** | |  | **Surname:** |  | | |
| **Position:** | |  | | | | |
| **Department/School:** | |  | | | | |
| **Staff ID Number:** | |  | **Telephone Number:** | | |  |
| **Email address:** | |  | | | | |
| **Reason access requested:** | | | | | | |
|  | | | | | | |
| **Access required to which parts of the system, if applicable e.g. system has different modules:** | | | | | | |
|  | | | | | | |
|  | | | | | | |
| I understand that during the course of my employment with the University I will have access to the personal data of University staff and students, visitors to University premises and other third parties whose data/images may be collected and processed through the **[system name]** system. I understand that I have a duty of confidentiality in relation to this personal information and as a University employee I am obliged to comply with the EU General Data Protection Regulation in 2016 and UK Data Protection Act 2018. I therefore undertake to:   * Only ever access and process personal information appropriately in order to carry out the duties attached to my post and for which I have been granted access to the **[system name]** system. * Never access or use any personal data for any purpose other than to perform the duties assigned to me. This includes viewing the data. * Never disclose any data verbally or in any other format to other University employees, students or representatives other than those who are authorised to have access to it in order to carry out their legitimate duties. * Never disclose any data verbally or in any other format to any third party, individual or organisation external to the University other than in accordance with [Data Protection legislation](https://ico.org.uk/) and the [University’s Data Protection Code of Practice](https://staff.napier.ac.uk/services/governance-compliance/governance/DataProtection/CodeofPractice/Pages/default.aspx). * Adhere to the obligations set out above and below during my period of employment and after it has ended. * Ensure that any data extracted or downloaded from the system and kept in any format is stored in University systems with the appropriate security whilst in use and [confidentially destroyed](https://staff.napier.ac.uk/services/governance-compliance/governance/DataProtection/Pages/DestructionofPersonalData.aspx) once the specific job for which it was required is complete. Retention or use for a longer period must be agreed with your Line Manager and/or [Governance Services](https://staff.napier.ac.uk/services/governance-compliance/Pages/who.aspx) and routine disposal of information must take place in accordance with your area’s [Records Retention Schedule](https://staff.napier.ac.uk/services/governance-compliance/governance/records/Pages/RecordsRetentionSchedules.aspx). * Attend Data Protection training prior to accessing the system and on a regular basis thereafter as required by the System Administrator in conjunction with School/Department management and Governance Services e.g. annually. * Report any breach or suspected breach of information security or data protection as required by the University’s [Data Protection Breach procedure](https://staff.napier.ac.uk/services/governance-compliance/governance/DataProtection/Pages/Breach-and-Incident-Reporting.aspx).   Further I understand that:   * I am bound by the University’s [Information Security Policies](http://staff.napier.ac.uk/services/cit/infosecurity/Pages/InformationSecurityPolicy.aspx), [Data Protection Policy and Code of Practice](https://staff.napier.ac.uk/services/governance-compliance/governance/DataProtection/Pages/default.aspx), [Manual Data Security Policy](https://staff.napier.ac.uk/services/governance-compliance/governance/DataProtection/Pages/SecurityofPersonalData.aspx), **[system name]** procedures and any other University policies and procedures, as updated from time to time, to which I have been directed or given a copy. I will familiarise myself with these policies and procedures before signing this form. * Disclosure or processing of personal information outside these terms must only ever take place in consultation with my Line Manager and/or Governance Services. * Any breach of my obligations as set out above may result in disciplinary action being taken against me. * If I have any queries about any aspect of the operation of the system or the above I will seek clarification from my Line Manager in the first instance. | | | | | | |
|  | | | | | | |
| **Signature:** |  | | | **Date:** |  | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Section 2 – to be completed by the applicant’s line manager or head of department/school** | | | |
|  | | | |
| I am satisfied that the above named member of staff is aware of their statutory obligations with regards to personal data and certify that they are an appropriate person to whom access to the **[system name]** System should be given. | | | |
|  | | | |
| **Signature:** |  | **Date:** |  |
| **Name:** |  | **Position:** |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Section 3 – to be completed by the system administrator** | | | | | |
|  | | | | | |
| **Access** | Approved | | Not Approved | | |
| **Reason:** |  | | | | |
| **Login name assigned to applicant:** | |  | | **Date:** |  |
| **Access/role allocated to applicant:** | | | | | |
|  | | | | | |
| **Signature:** |  | | **Date:** |  | |
| **Name:** |  | | **Position:** |  | |
| **Any further information relating to reasons access required or access permissions granted:** | | | | | |
|  | | | | | |

|  |
| --- |
| **Full links for information:** |
| Confidential Destruction:  [staff.napier.ac.uk/services/governance-compliance /governance/DataProtection/Pages/DestructionofPersonalData.aspx](http://staff.napier.ac.uk/services/secretary/governance/DataProtection/Pages/DestructionofPersonalData.aspx)  Data Protection Breach procedure:  <https://staff.napier.ac.uk/services/governance-compliance/governance/DataProtection/Pages/SecurityofPersonalData.aspx>  Data Protection Policy and Code of Practice: [staff.napier.ac.uk/services/ governance-compliance /governance/DataProtection/Pages/default.aspx](http://staff.napier.ac.uk/services/secretary/governance/DataProtection/Pages/default1.aspx)  Information Security Policies:  [staff.napier.ac.uk/services/cit/infosecurity/Pages/InformationSecurityPolicy.aspx](http://staff.napier.ac.uk/services/cit/infosecurity/Pages/InformationSecurityPolicy.aspx)  Manual Data Security Policy:  [staff.napier.ac.uk/services/ governance-compliance /governance/DataProtection/Pages/SecurityofPersonalData.aspx](http://staff.napier.ac.uk/services/secretary/governance/DataProtection/Pages/SecurityofPersonalData.aspx)  Records Retention Schedules:  [staff.napier.ac.uk/services/ governance-compliance /governance/records/Pages/RecordsRetentionSchedules.aspx](http://staff.napier.ac.uk/services/secretary/governance/records/Pages/RecordsRetentionSchedules.aspx) |