**Self-Assessment Questionnaire**

**Data Processors**

|  |  |  |  |
| --- | --- | --- | --- |
| **GDPR** | **GDPR**  **Self-Assessment Declaration providing guarantees that we will implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the rights of individuals:** | | |
| Name of Organisation |  | | |
| Notification Number(s)  (if notified) |  | | |
| Contact Number |  | | |
| Products and/or services provided |  | | |
| Number of sites/locations to be covered |  | | |
| Number of full time staff |  | Number of part-time staff |  |
| Name of Data Protection Officer |  | Number of sub-contractors **\*** |  |
| Date questionnaire completed |  | Completed by |  |

**A Introduction**

|  |  |
| --- | --- |
| Question 1 | |
| Are any of the individuals whose personal data you process on behalf of a data controller based in the EU? | Yes  No |

**B** **Data Collection**

|  |
| --- |
| Question 2 |
| What personal data are processed? (e.g. name, address, telephone number etc.) |
|  |

|  |
| --- |
| Question 3 |
| Why are these personal data processed? For what purpose are they used? |
|  |

|  |
| --- |
| Question 4 |
| Within the GDPR the term “special category data” replaces the existing term “sensitive personal data”. It also encompasses more data types than the current definition.  With the expanding definition in mind, is any special category data held or processed (e.g. medical/health data. Ethnic origin etc.)?  If so for what purpose? |
|  |
| **Personal data relating to criminal convictions and offences is subject to a separate EU legal instrument, known as the Law Enforcement Directive and this will impact on how organisations can process such data. These provisions will be written into new data protection legislation and further guidance as to how such data should be processes and protected, will be published in due course.** |

**C Governance**

|  |  |
| --- | --- |
| Question 5 | |
| Do you currently have a Data Protection Officer? | Yes  No |

|  |
| --- |
| Question 6 |
| If so, to whom does the Data Protection Officer report? |
|  |

|  |
| --- |
| Question 7 |
| What responsibility does the Data Protection Officer have? |
|  |

|  |  |
| --- | --- |
| Question 8 | |
| If you do not have a current Data Protection Officer, are you planning to appoint someone to such a role? | Yes  N/A  No |
| If you are not planning to appoint a Data Protection Officer, please explain the reason for not appointing | |
|  | |

|  |  |
| --- | --- |
| Question 9 | |
| Is there a written agreement in place between your organisation and Walsall College that outline how personal data should be processed? | Yes  No |
| **If yes, this agreement will require review against the new requirements with the GDPR, Data processors become accountable and liable under the GDPR and as such you ensure that the agreement has been updated.** | |

|  |
| --- |
| Question 10 |
| Is a central record of the processing activities you carry out on behalf of Walsall College maintained in a format that can be used to demonstrate Records of Processing activities to the Information Commissioners Office (ICO). ( see A.28 of the GDPR) |
|  |

**D Storage and Archiving**

|  |
| --- |
| Question 12 |
| How does your organisation store personal information on behalf of the data controller? (e.g. on computer or manual files or both and/or on personal devices?)  Set out details of databases/filing systems containing personal data. |
|  |

|  |
| --- |
| Question 13 |
| If information is stored on computer is this within the organisation or elsewhere? If elsewhere, identify the third party storing the data, detailing where and how the data are stored. |
|  |
| **If the data is being held by a third party, and the third party is acting as a sub-processor. Ensure you complete the Using Sub-Processors section of this self-assessment to assess this relationship.** |

|  |
| --- |
| Question 14 |
| If information is stored manually is this within the organisation or elsewhere? If elsewhere, identify the third party (sub-processor) storing the data, detailing where and how the data are stored. |
|  |
| **If your data is being held by a third party, the third party is acting as a sub-processor. Ensure you complete the Using Sub-Processors section of this self-assessment to assess their relationship.** |

|  |
| --- |
| Question 15 |
| If your organisation processes special category personal data on behalf of a data controller, is such data stored separately from any other personal data or subject to any specific marking, security or handling rules/restrictions? |
|  |

|  |
| --- |
| Question 16 |
| In what format or in what medium is archived information stored? |
|  |

|  |
| --- |
| Question 17 |
| Where is archived information stored? If it is stored on third party premises, identify that third party and where and how it is stored? |
|  |
| **If data is being held by a third party the third party is acting as a sub-processor. Ensure you complete the Using Sub-Processors section of this self-assessment to assess this relationship.** |

**E Security**

|  |
| --- |
| Question 18 |
| Describe and outline the security procedure in operation in your organisation to keep all information processed on behalf of a data controller secure. Describe the physical, administrative and technological procedures used that are relevant to the data you process |
|  |

|  |
| --- |
| Question 19 |
| Who has access to personal information within the organisation/outside the organisation? |
|  |

|  |
| --- |
| Question 20 |
| Who authorises such access? |
|  |

|  |
| --- |
| Question 21 |
| Do you have policies and procedures in place for detecting and dealing with breaches? If so, what are they? |
|  |

|  |
| --- |
| Question 22 |
| How do you check that there has been no internal unauthorised access to personal data? What data audit facilities/mechanisms are in place? |
|  |

|  |
| --- |
| Question 23 |
| Do you have policies and procedures in place to report breaches to Walsall College? If so, what are they? |
|  |
| **Under GDPR, certain data breaches will need to be reported to the Commissioner’s Office within 72 hours of discovery, by the data controller. Data processors will need to ensure they communicate any breaches or compromises of data to the data controller as soon as possible.** |

**F Destruction of Data and Termination of Contract**

|  |  |
| --- | --- |
| Question 24 | |
| Under your agreement with Walsall College, are you responsible for the destruction of the data? | Yes  N/A  No |

|  |
| --- |
| Question 25 |
| If yes to Q24, how is personal information destroyed? |
|  |

|  |
| --- |
| Question 26 |
| Who authorises destruction? Who carries out destruction? What agreement are in place with contractors who provide shredding facilities/services? |
|  |

|  |
| --- |
| Question 27 |
| Are there clear instructions in the contract detailing what happens to the data at the end of the contract period |
|  |

**G Using Sub-Processors**

|  |
| --- |
| Question 28 |
| Are any of your processing activities carried out by third parties (sub-processors)?  List them and describe the processes and location of the provider and the data. |
|  |

|  |
| --- |
| Question 29 |
| Who authorises these processing activities? How will you ensure that you obtain written authorisation from Walsall College ? |
|  |
| **Article 28 states that a data processor shall not engage in the services of another data processor as a sub-processor without prior specific or general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes?** |

|  |
| --- |
| Question 30 |
| Are written agreements in place covering these sub processing arrangements? |
|  |
| **Each agreement will require review against the new requirement within the GDPR. Data processors become accountable and liable under the GDPR and as such, require extra information from data controllers to ensure they are compliant.**  **Data processors engaging in the services of a sub-processor will also need to ensure sufficient guarantee of compliance is given by the sub-processor. In the event of a breach or data compromise, should the service of a sub-processor been contacted by a data processor, the data processor will hold liability for this,** |

|  |
| --- |
| Question 31 |
| Outline the security measures under which each sub-processor is required to operate |
|  |

|  |
| --- |
| Question 32 |
| Do the sub-processors used by your organisation use any other organisation to perform that service on their behalf? If so, list the organisation and any written arrangements in place with regards to the service these sub-contractors offer. |
|  |
| **Under the GDPR if a data processor employ another processor to perform a service on behalf of a data controller they should obtain either general or specific written authorisation. The data processor, with which the data controller has its agreement with, remains liable for the actin of any data processor to which it sub-contracts.** |

**H Transfers of Personal Data**

|  |
| --- |
| Question 33 |
| Do you transfer data   1. cross-departmentally: and/or 2. to third parties outside the organisation |
|  |

|  |
| --- |
| Question 34 |
| How is data transferred? (e.g. encrypted email? Secure fax?) |
|  |

|  |
| --- |
| Question 35 |
| In what countries are those people to whom you disclose information (whether inside the organisation or external) located? |
|  |

|  |
| --- |
| Question 36 |
| Where data is transferred outside the EU, what measures are used to ensure compliance with the requirements under GDPR relating to Transfers of personal data to third countries or international organisations? Articles 44 – 50 of the GDPR |
|  |

**I Training**

|  |
| --- |
| Question 37 |
| Do the employees in your organisation receive regular training on data protection and other relevant law? If so, please describe the nature of the training given and identify who is responsible for carrying out the training |
|  |

|  |
| --- |
| Question 38 |
| Are refresher courses held/ If so, please describe the nature of the training given, where it is given, identify who is responsible for carrying out the training and who is directed to attend. |
|  |

|  |
| --- |
| Question 39 |
| Are staff aware that unlawful access to and/or disclosure of personal data is prohibited? |
|  |

|  |
| --- |
| Question 40 |
| Have the following attended a GDPR awareness session?   1. The Board  Yes  No  N/A 2. Senior Management  Yes  No  N/A 3. Security/IT Team  Yes  No  N/A 4. All other staff  Yes  No  N/A |

**\*If data is being held by a third party the third party is acting as a sub-processor. Ensure you complete the Using Sub-Processors section of this self-assessment to assess this relationship**