**APPENDIX 4: DATA PROTECTION SCREENING QUESTIONNAIRE**

The Council takes its data protection obligations very seriously and is committed to the protection of personal data throughout the supply chain.  We, therefore, require any partners and suppliers who process personal data belonging to the Council, to do so in accordance with the Data Protection Act 2018 and UK General Data Protection Regulations.

The following questions seek to establish your current policies, procedures, and practice for Information Governance.  All questions must be answered in full but may reference documents or policies of your organisation which you may be asked to provide.

|  |  |
| --- | --- |
| Question 1: About your service | Supplier Response |
| (a) Organisation name |  |
| (b) Name and contact details of the organisation’s Data Protection lead |  |
| (c) Thinking specifically about the personal data you come into contact with, on behalf of Bath and North East Somerset Council, do you consider yourself to be the (select one):(i) Sole Data Controller for the data(ii) Joint Data Controller(iii) Data Processor(iv) I am unclear about these terms |  |
| (d) What sort of personal data do you process on behalf of the council?  Please include personal data and special category data (eg young peoples’ names, DoBs, contact details and medical conditions) |  |
| (e) Please provide a brief overview of what the service is that you are providing |  |
| Question 2: Software systems |  |
| (a) Do you use any electronic software systems to process the data?  For example Microsoft office products or a bespoke system.If you only rely on paper-based records, please continue to Question 4. |  |
| (b) Please list the electronic systems you use |  |
| (c) For any systems, with the exception of the Microsoft Office suite, please provide the weblink to their website |  |
| (d) For all electronic systems, what controls are in place to ensure access is restricted only to employees who should have access to the data? |  |
| (e) In what country does the software provider host their system?  NB “EU” is not an adequate response. |  |
| Question 3: Information security |  |
| (a) What is your organisation’s network password policy (length of password, different characters, frequency of changes)? |  |
| (b) In what country is your server based?  Nb “EU” is not an adequate response. |  |
| (c) Please provide any further information that demonstrates the technical security measures you have in place, for example if you have Cyber Essentials certification or ISO27000/1 accreditation. |  |
| Question 4: Paper records |  |
| For paper-based records, how are these stored and secured?  Please also detail how access is restricted to those who need access. |  |
| Question 5: Retention and disposal |  |
| (a) How do you dispose of your electrical assets (eg computers, external drives)? |  |
| (b) How do you dispose of your paper records? |  |
| Question 6: Staff training |  |
| (a) How frequently are staff who handle personal data expected to attend data protection training? |  |
| (b) How is your data protection training provided (eg external provider, internal training)? |  |
| (c) What percentage of staff who handle Bath and North East Somerset Council personal data have:(i) DBS clearance(ii) Enhanced DBS clearance(nb this percentage should be based on headcount, and not FTE) |  |
| Question 7: Policies |  |
| When were your following policies last reviewed?  If you don’t have them, just write “N/A”.  Please note, we may ask to see a copy of some policies (you will be contacted separately if this is the case). |  |
| (a) Data Protection Policy |  |
| (b) Information Security Policy |  |
| (c) Acceptable Usage Policy |  |
| (d) Records Management Policy |  |
| (e) Retention Schedule |  |

The council’s Data Protection team will consider your responses and advise the contract manager whether we consider your answers to provide adequate assurances.  Agreements must not begin until this assessment has been concluded, so it is in your best interest to ensure all questions are answered as fully and promptly as possible.

**GLOSSARY**

**As defined by the UK General Data Protection Regulation**

1. **Processing, *art.4(2), UK GDPR***
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.**
3. **Personal Data, art.4(1), UK GDPR**
4. **Personal data means any information relating to an identified or identifiable natural person (‘data subject’).**
5. **An identifiable natural person is one who can be identified, directly or indirectly, in particular by any 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.**
6. **Special Categories of Personal Data, art.9, UK GDPR**
7. **Special Categories of Personal Data refers to personal data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life.**

**SCORING MATRIX**

Each of the questions will be assessed using the following scoring matrices.  The council reserves the right to exclude any organisation assessed as High Risk on any of the above questions.

|  |  |
| --- | --- |
| **Question 1: About your service****Not scored** | **Scoring Matrix Description** |
| (a) Organisation name | N/A |
| (b) Name and contact details of the organisation’s Data Protection lead | N/A |
| (c) Thinking specifically about the personal data you come into contact with, on behalf of Bath and North East Somerset Council, do you consider yourself to be the (select one):(i) Sole Data Controller for the data(ii) Joint Data Controller(iii) Data Processor(iv) I am unclear about these terms | If the supplier considers themselves to be a sole Data Controller, the remainder of this questionnaire is not necessary.These questions are designed to evaluate how much and how sensitive the personal data involved in the contract is.  The responses given here should not be scored, but will give the Information Governance team an indicator of the level of assurances required from the contract. |
| (d) What sort of personal data do you process on behalf of the council?  Please include personal data and special category data (eg young peoples’ names, DoBs, contact details and medical conditions) |
| (e) Please provide a brief overview of what the service is that you are providing |
| **Question 2: Software systems****Maximum score: 2** | **Acceptable, no concerns (2 points)** | **Medium Risk, some concerns (1 point)** | **High Risk, significant concerns (0 points)** |
| (a) Do you use any electronic software systems to process the data?  For example Microsoft office products or a bespoke system.If you only rely on paper-based records, please continue to Question 4. | Familiar with all software systems in place / no electronic processing.Access controls, restricted to only those employees working on B&NES data.UK-based cloud systems. | List only includes the main operating systems (eg Microsoft or Google packages), or a non-exhaustive list.Main network access controls only; all employees could access B&NES data.Data hosted outside the UK but within the EU. | Supplier is unaware of all the systems in place.No clear access controls.No detail provided about the systems.Unclear about hosting arrangements or hosted outside of the EU. |
| (b) Please list the electronic systems you use |
| (c) For any systems, with the exception of the Microsoft Office suite, please provide the weblink to their website |
| (d) For all electronic systems, what controls are in place to ensure access is restricted only to employees who should have access to the data? |
| (e) In what country does the software provider host their system?  Nb “EU” is not an adequate response. |
| **Question 3: Information security****Maximum score: 9** | **Acceptable, no concerns (3 points)** | **Medium Risk, some concerns (1 point)** | **High Risk, significant concerns (0 points)** |
| (a) What is your organisation’s network password policy (length of password, different characters, frequency of changes)? | Minimum of 14 characters; combination of uppercase, lowercase, numbers, special characters; “Password for life”; lock outs after three incorrect password attempts. | Minimum of 12 characters; combination of at least two from uppercase, lowercase, numbers and special characters; monthly changes; lock-outs after less than eight incorrect password attempts. | No password policy, and no controls if the password is incorrectly entered |
| (b) In what country is your server based?  Nb “EU” is not an adequate response. | UK | Outside the UK, but within the EU | Outside the EU with no clear controlsUnknown |
| (c) Please provide any further information that demonstrates the technical security measures you have in place, for example if you have Cyber Essentials certification or ISO27000/1 accreditation. | Accreditation to ISO27000/1, achieved the NHS DSP Toolkit, or other information security standardsEncryption method fully explained.  Make/brand of encryption software detailed.  Details of FIPS/NCSC/CAPS product accreditation | Working towards one of the recognised information security standardsEncryption in place with other secure connections details (e.g. PGP connections) but no specific product details supplied.   | None |
| **Question 4: Paper records****Maximum score: 2** | **Acceptable, no concerns (2 points)** | **Medium Risk, some concerns (1 point)** | **High Risk, significant concerns (0 points)** |
| For paper-based records, how are these stored and secured?  Please also detail how access is restricted to those who need access. | Site secured, CCTV and alarmedLocked storageAccess restricted only to those who need to beFire-proofFire suppression measures in placeOR No paper records | Paper records stored in secured building, with access only to employeesFire suppression measures in place | No security or fire provision arrangements considered |
| **Question 5: Retention and disposal****Maximum score: 4** | **Acceptable, no concerns (2 points)** | **Medium Risk, some concerns (1 point)** | **High Risk, significant concerns (0 points)** |
| (a) How do you dispose of your electrical assets (eg computers, external drives)? | Third parties, NCSC-approved products used to erase all data | Using a reputable destruction company, but no NCSC approval checked | No recorded methods of destruction, or insufficient methods |
| (b) How do you dispose of your paper records? | Cross-cut shred or certified third party contractor | Using a reputable destruction company, but no certificates of destruction | No recorded methods of destruction, or insufficient methods |
| **Question 6: Staff training****Maximum score: 6** | **Acceptable, no concerns (2 points)** | **Medium Risk, some concerns (1 point)** | **High Risk, significant concerns (0 points)** |
| (a) How frequently are staff who handle personal data expected to attend data protection training? | Annually | Biennially | Never / only at start of employment |
| (b) How is your data protection training provided (eg external provider, internal training)? | Certified trainer / training course | Provided in-house by someone with a good understanding of data protection | None / non-certified online resources |
| (c) What percentage of staff who handle Bath and North East Somerset Council personal data have:(i) DBS clearance(ii) Enhanced DBS clearance(nb this percentage should be based on headcount, and not FTE) | (i) 100%(ii) 80%+ | (i) 80% - 99%(ii) 50% - 79% | (i) >80%(ii) >50% |
| **Question 7: Policies****Maximum score: 10** | **Acceptable, no concerns (2 points)** | **Medium Risk, some concerns (1 point)** | **High Risk, significant concerns (0 points)** |
| When were your following policies last reviewed?  If you don’t have them, just write “N/A”.  Please note, we may ask to see a copy of some policies (you will be contacted separately if this is the case). |  |  |  |
| (a) Data Protection Policy | Within the past 12 months | Within the past 24 months, with a review planned | Don’t have one or more than two years ago |
| (b) Information Security Policy | Within the past 12 months | Within the past 24 months, with a review planned | Don’t have one or more than two years ago |
| (c) Acceptable Usage Policy | Within the past 12 months | Within the past 24 months, with a review planned | Don’t have one or more than two years ago |
| (d) Records Management Policy | Within the past 24 months | Don’t have one or more than two years ago | N/A |
| (e) Retention Schedule | Within the past 12 months | Within the past 24 months, with a review planned | Don’t have one or more than two years ago |

**Total scores (out of 33):**

Acceptable, no concerns = 25 or more, with a score of more than 5 from question 3

Medium Risk, some concerns = 16 – 24, with a score of at least 3 from question 3

High Risk, significant concerns = 15 or less OR a score of less than 3 from question 3