**The Arch Medical Practice**

**Data Protection Impact Assessment.**

The person(s) conducting a full DPIA must have a clear knowledge of the project and proposed uses of information and technology, working closely with identified stakeholders, staff and others with expert knowledge of the project and solutions. This may include third party suppliers.

This process supports Article 29 of the General Data Protection Regulation

**Section 1 – Project Information and Contact Details**

|  |  |
| --- | --- |
| **Project name** |  |
| **Describe the project background, why has the project been initiated?** Describe the new project or product, including the data processing activity associated with it. |  |
| **Benefit** The expected benefits for the organisation, data subjects, society in general. |  |
| **Describe the constraints to the project:** |  |
| **Estimated completion date of the project:** |  |

**Details of the Project Lead**

|  |  |
| --- | --- |
| Name |  |
| **Job Title** |  |
| **Department** |  |
| **Telephone** |  | **Email** |  |

**Details of the Information Asset Owner**

|  |  |
| --- | --- |
| Name |  |
| **Job Title** |  |
| **Department** |  |
| **Telephone** |  | **Email** |  |

**Section 2 - Lawfulness of Processing**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **L1** | **The information processed is about:** | Employees | ☐ | Patients | ☐ |
| Students | ☐ | Business partners or organisations | ☐ |
| Other – provide details |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **L2** | **The sources of information are:** | Obtained from the individual  | ☐ | Obtained from another source | ☐ |
| Publicly available | ☐ | Business partners or organisations | ☐ |
| Other – provide details |

**L3. Does the project include any of the following data sets?**

|  |  |
| --- | --- |
| Personal Identifiable details (e.g. name, address, postcode, data of birth) | ☐ |
| Identifier numbers (e.g. NHS, national insurance, passport, driving license) | ☐ |
| Family, lifestyle and social circumstances (e.g. marital status, housing, travel, leisure activities, membership of charities) | ☐ |
| Education and training details (e.g. qualifications or certifications, training records) | ☐ |
| Employment details (e.g. career history, recruitment and termination details, attendance details, appraisals) | ☐ |
| Financial details (e.g. banking, income, salary, assets, investments, payments) | ☐ |
| Goods or services (e.g. contracts, licenses, agreements) | ☐ |
| Legal details (e.g. legal documents or agreements, court papers) | ☐ |
| Technology identifiers (e.g. device names, applications, tools, protocols, such as IP addresses, cookie identifiers, radio frequency identification tags) | ☐ |
| Location data (e.g. GPS location, Wi-Fi tracking, vehicle tracking) | ☐ |

**L4. What is the legal basis for processing personal information?**

|  |  |  |
| --- | --- | --- |
| 6(1)(a) | Consent of the data subject | ☐ |
| 6(1)(b) | Processing is necessary for the performance of a contract to which the data subject is party…. | ☐ |
| 6(1)(c) | Processing is necessary for compliance with a legal obligation | ☐ |
| 6(1)(d) | Processing is in the vital interests of the data subject  | ☐ |
| 6(1)(e) | Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller | ☐ |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **L4. What is the legal basis for processing special categories of personal information?** For each special category of personal data being processed at least one of the conditions below must apply. | racial or ethnic origin | political opinions | religious or philosophical beliefs | trade union membership | health or sex life and sexual orientation | genetic data  | biometric data  |
| 9(2)(a)  | Explicit consent of the data subject | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 9(2)(b) | Carrying out of obligations under employment, social security or social protection law, or a collective agreement | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 9(2)(c)  | Vital interests of a data subject who is physically or legally incapable of giving consent. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 9(2)(d)  | Processing by a not-for-profit body with a political, philosophical, religious or trade union aim. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 9(2)(e)  | Data manifestly made public by the data subject | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 9(2)(f)  | Establishment, exercise or defence of legal claims or where courts act in their judicial capacity | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 9(2)(g)  | Necessary for reasons of substantial public interest | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 9(2)(h)  | Necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services. | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 9(2)(i)  | Necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |

|  |  |  |  |
| --- | --- | --- | --- |
| **L5** | **Consent requires a positive action by the individual, rather than being assumed as the default. Consent is obtained through:** | Written Process |  |
| Verbal Process |  |

|  |  |  |
| --- | --- | --- |
| **L6** | **Explain how consent will be collected and recorded?**  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **L7** | **Can individuals withdraw or opt-out from their data being processed?** | Yes □ | No □ |

|  |  |  |
| --- | --- | --- |
| **L8** | **How will the withdrawal or opt-out be managed and records?**  |  |

|  |  |
| --- | --- |
| **L5 – L8** **not applicable**  |   |

|  |  |  |  |
| --- | --- | --- | --- |
| **L9** | **Will a Privacy Notice be provided or made available to individuals prior to the collection of data?** | Yes □ | No □ |

|  |  |  |
| --- | --- | --- |
| **L10** | **The data will be used for the following purposes:** |  |

|  |  |  |
| --- | --- | --- |
| **L11** | **Are potential new purposes likely to be identified as the scope of the project expands? If so, describe what these are.**  |  |

|  |
| --- |
| **L10. When Data is obtained directly from data subject confirm that the following information has been included in the Privacy Notice.** |
| Identity and contact details of the controller and where applicable, the controller’s representative and the data protection officer | Yes □ | No □ |
| Any recipient or categories of recipients of the personal data | Yes □ | No □ |
| Purpose of the processing and the lawful basis for the processing | Yes □ | No □ |
| Details of transfers to third country and safeguards | Yes □ | No □ |
| Retention period or criteria used to determine the retention period | Yes □ | No □ |
| The existence of data subject’s rights | Yes □ | No □ |
| The right to withdraw consent at any time, where relevant | Yes □ | No □ |
| The right to lodge a complaint with a supervisory authority | Yes □ | No □ |
| Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data | Yes □ | No □ |
| The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences. | Yes □ | No □ |

|  |
| --- |
| **L11. When Data has not been obtained directly from data subject confirm that the following information has been included in the Privacy Notice.** |
| Identity and contact details of the controller and where applicable, the controller’s representative and the data protection officer | Yes □ | No □ |
| Purpose of the processing and the lawful basis for the processing | Yes □ | No □ |
| Categories of personal data | Yes □ | No □ |
| Any recipient or categories of recipients of the personal data | Yes □ | No □ |
| Details of transfers to third country and safeguards | Yes □ | No □ |
| Retention period or criteria used to determine the retention period | Yes □ | No □ |
| The existence of data subject’s rights | Yes □ | No □ |
| The right to withdraw consent at any time, where relevant | Yes □ | No □ |
| The right to lodge a complaint with a supervisory authority | Yes □ | No □ |
| The source the personal data originates from and whether it came from publicly accessible sources | Yes □ | No □ |
| The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences. | Yes □ | No □ |

|  |  |  |
| --- | --- | --- |
| **L12** | **Privacy Notices have not yet been produced** |   |

**Section 3 Data Quality**

|  |  |  |
| --- | --- | --- |
| **D1** | **Who will be able to access the data? Include internal users, third parties, business partners etc.** |   |

|  |  |  |
| --- | --- | --- |
| **D2** | **Who will be record or input the data? Include internal users, third parties, business partners etc.** |   |

|  |  |  |
| --- | --- | --- |
| **D3** | **Who will be able to amend the data? Include internal users, third parties, business partners etc.** |   |

|  |  |  |
| --- | --- | --- |
| **D4** | **What training will the users receive for accessing, inputting or amending the information or data?** |   |

|  |  |  |  |
| --- | --- | --- | --- |
| **D5** | **Will the information be checked for accuracy?** | Yes □ | No □ |

|  |  |
| --- | --- |
| **D6** | **Have you defined a standard operating procedure covering the following activities?** |
| Revoking and approving user access to the data | Yes □ | No □ |
| Developing and maintaining staff competences for record keeping and data quality | Yes □ | No □ |
| Ensuring timely, accurate and complete recording of data | Yes □ | No □ |
| Addressing and escalating data quality issues in a timely manner | Yes □ | No □ |
| Consideration of compliance with legislation and local procedures | Yes □ | No □ |
| Ensuring all data is handled in a secure and confidential way | Yes □ | No □ |
| Correcting or merging data inaccuracies | Yes □ | No □ |
| The erasure, blocking of data | Yes □ | No □ |

|  |  |  |
| --- | --- | --- |
| **D7** | **Describe the steps which shall be taken to ensure that the information is accurate, complete and up-to-date:** |   |

**Section 4 Supplier Overview**

|  |  |  |
| --- | --- | --- |
| **S1** | **What is the name of the supplier company?** |  |

|  |  |  |
| --- | --- | --- |
| **S2** | **Is the supplier a subsidiary company? If so enter the name of the parent company?** |  |

|  |  |
| --- | --- |
| **S3** | **Does the parent company have the power to hold the subsidiary company accountable for its performance?** |
| **Yes** |  | The remaining questions must be completed for the parent company |
| **No** |  | The remaining questions must be completed for the subsidiary company |

|  |  |  |
| --- | --- | --- |
| **S4** | **What is the company’s registered address?** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **S5** | **Is the company data protection registered with a supervisory authority such as the ICO? If so provide details of the registration.** | **Supervisory Authority Name:** |  |
| **Registration Number:** |  |

|  |  |  |
| --- | --- | --- |
| **S6** | **Has the company appointed a data protection officer? Provide the DPO contact details.** |  |

|  |  |  |
| --- | --- | --- |
| **S7** | **Has the company attained any certifications, seals or marks to demonstrate compliance with data protection law? Is so, provide details.** |  |

|  |  |  |
| --- | --- | --- |
| **S8** | **Is information security training provided to supplier employees on a regular basis? If so provide details.** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **S9** | **Is the company registered and compliant with the Department of Health’s Data Security & Protection Toolkit (formally known as the IG Toolkit)?** | **Registration Number** |  |
| **Score** |  |

|  |  |
| --- | --- |
| **S10** | **Has the company attained any of the listed standards:** |
| ISO27001: Information Security Management, if so please obtain a copy of the certification | Yes □ | No □ |
| ISO29100: Privacy Framework Standard, if so please obtain a copy of the certification | Yes □ | No □ |
| Cyber Essentials (CE) or Plus (CE+) certification | Yes □ | No □ |
| UK Digital Marketplace | Yes □ | No □ |
| Cloud Computing Standards : Only applicable to remote server developments | Yes □ | No □ |

|  |  |  |  |
| --- | --- | --- | --- |
| **S11** | **Does the main contract include Data Protection and Freedom of Information provisions?** | Yes □ | No □ |

|  |  |
| --- | --- |
| **S1 – S11** **not applicable**  |   |

**Section 5 Technical and Security Measures**

|  |  |  |
| --- | --- | --- |
| **T1** | **What business continuity plans are in place in case of data or damage? (As a result of human error, virus, network failure, theft, fire, floods etc.)** |  |

|  |  |  |
| --- | --- | --- |
| **T2** | **What physical security measures have been undertaken to protect the data from unauthorised access, alteration or destruction?**  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **T3** | **Is there a usable audit trail in place for the use of the data? If yes, what data will be captured and how will it be stored?** | Yes □ |  |
| No □ |

|  |  |  |  |
| --- | --- | --- | --- |
| **T4** | **Is the use of technology being considered? If yes, provide details of the internal ICT department stakeholder involved?** | Yes □ |  |
| No □ |

|  |  |  |  |
| --- | --- | --- | --- |
| **T5** | **Is the technology supported by the supplier or internal ICT department?** | Supplier |  |
| ICT Department |  |
| Neither |  |

|  |  |  |
| --- | --- | --- |
| **T6** | **What are the technical security measures have been undertaken to protect the data from destruction and loss?** |  |

|  |  |  |
| --- | --- | --- |
| **T7** | **What are the technical security measures have been undertaken to protect the data from alteration?** |  |

|  |  |  |
| --- | --- | --- |
| **T8** | **What are the technical security measures have been undertaken to protect the data from unauthorised disclosure or access?** |  |

|  |  |
| --- | --- |
| **T1 – T8** **not applicable**  |   |

|  |  |  |  |
| --- | --- | --- | --- |
| **T9** | **Is the use of cloud technology being considered? If yes, provide the data centre location.** | Yes □ |  |
| No □ |

|  |  |  |  |
| --- | --- | --- | --- |
| **T10** | **Is the cloud technology supported by the supplier** | Yes □ | No □ |

|  |  |  |  |
| --- | --- | --- | --- |
| **T11** | **Does the cloud hosting data centre(s) meet any standards such as tier-x standards to demonstrate cloud security? If so, provide details.** | Yes □ |  |
| No □ |

|  |  |  |  |
| --- | --- | --- | --- |
| **T12** | **Could the cloud technology change the way data is stored?** | Yes □ | No □ |
| **T13** | **How will the organisation be alerted to any possible cloud breaches?** |  |

|  |  |
| --- | --- |
| **T8 – T13** **not applicable**  |   |

|  |  |  |  |
| --- | --- | --- | --- |
| **T14** | **Is the use of payment processing technology being used or considered? If yes, provide details of the internal financial services stakeholder involved?** | Yes □ |  |
| No □ |

|  |  |  |  |
| --- | --- | --- | --- |
| **T15** | **Is the use of payment processing technology supported by the supplier?** | Yes □ | No □ |

|  |  |  |  |
| --- | --- | --- | --- |
| **T16** | **Is the use of mobile devices being considered? If yes, provide details.** | Yes □ |  |
| No □ |

|  |  |  |  |
| --- | --- | --- | --- |
| **T17** | **Are the mobile devices supported by the supplier or internal ICT department?** | Supplier |  |
| ICT Department |  |
| Neither |  |

|  |  |  |
| --- | --- | --- |
| **T18** | **How will users escalate cyber security, data security or data breaches in a timely manner?** |  |

**Section 6 Systematic Monitoring, Automated Decisions and Profiling**

|  |  |  |  |
| --- | --- | --- | --- |
| **S1** | **Is the use of surveillance or CCTV being considered?** | Yes □ | No □ |

|  |  |  |  |
| --- | --- | --- | --- |
| **S2** | **The aim of the surveillance or CCTV is:** | Protection of human life and health |  |
| Protection of property |  |
| Protection of employee life and health |  |
| Control over entry and exit from official business premises |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **S3** | **Are there any other aims of the surveillance or CCTV?** | Control over employees |  |
| Ascertaining diligence at work |  |
|  | Other | *[Please provide details]* |

|  |  |
| --- | --- |
| **S4** | **Have you prepared the following:** |
| Public notifications which are comprehensive, visible, positioned at the point the individual comes under surveillance | Yes □ | No □ |
| Employee notifications which detail the surveillance in the official business premise | Yes □ | No □ |
| Adoption of a policy regulating the manner of performing surveillance | Yes □ | No □ |
| That no surveillance is used in dressing rooms, fitting rooms, toilets and bathrooms and other similar areas | Yes □ | No □ |

|  |  |
| --- | --- |
| **S5** | **Does the public and employee notification contains:** |
| When surveillance is being performed | Yes □ | No □ |
| Details of the controller performing the surveillance | Yes □ | No □ |
| The purposes and period of preserving the images and recordings | Yes □ | No □ |

|  |  |  |
| --- | --- | --- |
| **S6** | **What is the retention period for the surveillance images and recordings?** |  |

|  |  |
| --- | --- |
| **S1-S6** **not applicable**  |   |

|  |  |  |  |
| --- | --- | --- | --- |
| **S7** | **Is the use of systematic monitoring of individuals being considered** | Yes □ | No □ |

|  |  |  |
| --- | --- | --- |
| **S8** | **If systematic monitoring is being considered, please provide details of the monitoring that will take place including who, what, why and how often:** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **S9** | **Is the use of systematic monitoring outcome involving decision making?** | Yes □ | No □ |

|  |  |  |
| --- | --- | --- |
| **S10** | **If decision-making is envisaged, please provide details** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **S11** | **If decision-making is envisaged, will this interfere with the individual’s freedom and rights?** | Yes □ | No □ |

|  |  |
| --- | --- |
| **S12** | **If systematic monitoring is being considered, have you prepared a document detailing the following?**  |
| Who will be monitored | Yes □ | No □ |
| Why the monitoring will be conducted | Yes □ | No □ |
| When the monitoring will be conducted | Yes □ | No □ |
| Where monitoring will be conducted | Yes □ | No □ |
| What will be looked for when conducting monitoring | Yes □ | No □ |
| How to conduct monitoring | Yes □ | No □ |
| Where the monitoring data will be stored | Yes □ | No □ |
| Who will access the monitoring data | Yes □ | No □ |
| Details of any decision-making from process | Yes □ | No □ |

|  |  |
| --- | --- |
| **S7-S12** **not applicable**  |   |

|  |  |  |  |
| --- | --- | --- | --- |
| **S13** | **Is automated decision-making without human intervention being considered?** | Yes □ | No □ |

|  |  |  |  |
| --- | --- | --- | --- |
| **S14** | **If automated decision-making is envisaged, will it concern children or special categories of data?** | Yes □ | No □ |

|  |  |
| --- | --- |
| **S15** | **If automated decision-making is being considered, is the individual able to:**  |
| Obtain human intervention | Yes □ | No □ |
| Express their point of view | Yes □ | No □ |
| Obtain an explanation of the decision and challenge it | Yes □ | No □ |

|  |  |
| --- | --- |
| **S16** | **If automated decision-making is being considered, is this due to any of the following conditions?** |
| Necessary for entering into or performance of a contract between you and the individual | Yes □ | No □ |
| Is authorised by law\* | Yes □ | No □ |
| \*Law details: |  |
| Based on explicit consent | Yes □ | No □ |

|  |  |
| --- | --- |
| **S13-16** **not applicable**  |   |

|  |  |
| --- | --- |
| **S17** | **Will the evaluation ‘profiling’ of certain personal aspects of an individual be carried out, such as:**  |
| Performance at work | Yes □ | No □ | Reliability | Yes □ | No □ |
| Economic situation | Yes □ | No □ | Behaviour | Yes □ | No □ |
| Health | Yes □ | No □ | Location | Yes □ | No □ |
| Personal preferences | Yes □ | No □ | Movements | Yes □ | No □ |
| Other |  |

|  |  |  |
| --- | --- | --- |
| **S18** | **If profiling is envisaged, please provide details of the mathematical or statistical procedures for the profiling:** |  |

|  |  |
| --- | --- |
| **S17-18** **not applicable**  |   |

**Section 7 Disclosing and Sharing**

|  |  |  |  |
| --- | --- | --- | --- |
| **D1** | **Will the project facilitate the transferring or disclosing information to a country or territory outside of the European Economic Area?** | Yes □ | No □ |

|  |  |  |  |
| --- | --- | --- | --- |
| **D2** | **Will the project by any means disseminate information with third parties?** | Yes □ | No □ |

|  |  |  |  |
| --- | --- | --- | --- |
| **D3** | **If a third-party disclosure is required has a non-disclosure agreement (NDA) been established?** | Yes □ | No □ |

|  |  |  |  |
| --- | --- | --- | --- |
| **D4** | **Will the project by any means require the sharing of personal information?** | Yes □ | No □ |

|  |  |  |  |
| --- | --- | --- | --- |
| **D5** | **If the sharing of personal information is envisaged has an information sharing agreement been established between the discloser and recipients?** | Yes □ | No □ |

|  |  |  |  |
| --- | --- | --- | --- |
| **D6** | **Will any information be published on the internet or in other media types? If yes, please provide details:** | Yes □ | No □ |

|  |  |  |  |
| --- | --- | --- | --- |
| **D8** | **Will the project involve direct marketing?** | Yes □ | No □ |

The ***Data Privacy Impact Assessment Form*** must now be returned completed and signed to the Date Protection Officer who will review the form and identify any privacy risks and proposed solutions and/or mitigating actions in Section 8.

**Completed by:** Project Lead

Name ………………………………………………………………………………………………..…

Signature...........................................................................Date …………………………………

## Section 8 – Privacy issues identified and risk analysis

### Identify the privacy and related risks (see Appendix 1 for further information)

### *NB. By allocating a reference number to each identified privacy issue will ensure you link back to this throughout the rest of the assessment. Column (a), (b) and/or (c) must be completed for each privacy issue identified.*

| **Ref No.**  | **Privacy issue –** element of the initiative that gives rise to the risk | 1. **Risk to individuals** *(complete if appropriate to issue or put not applicable)*
 | 1. **Compliance risk**
* *(complete if appropriate to issue or put not applicable)*
 | 1. **Associated organisation/corporate risk** *(complete if appropriate to issue or put not applicable)*
 |
| --- | --- | --- | --- | --- |
| *PR1* | *Individuals are not aware of the initiative as no communication materials have been planned* | *Individuals not aware that their data is being processed*  | *Non-compliance with DPA principle 1 – fair and lawful processing* | 1. *May lead to public mistrust*
2. *May lead to sanction by the Information Commissioners office (ICO)*
 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

### Identify the privacy solutions

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Risk – taken from column (a), (b) and/or (c) in table 1.** | **Risk score – see tables at Appendix 2** | **Proposed solution(s)/mitigating action(s)** | **Result:** is the risk accepted, eliminated, or reduced? |
| **Likelihood** | **Impact** | **RAG status** |  |  |
| ***PR1*** | *Individuals not aware that their data is being processed. Non-compliance with DPA principle 1 – fair and lawful processing**1. May lead to public mistrust**2. May lead to sanction by the Information Commissioners office (ICO)* | **5** | **5** | **R** | *Communication plan to be developed to ensure compliance with fair and lawful processing**Assurance that there will be an active communication campaign* *All relevant staff informed of need to understand and disseminate communication material.* | *Reduced to an acceptable level (it is not possible to eliminate at this stage as the Communications plan will need to ensure it addresses all aspects to enable individuals to be fully informed).* |
|  |  |  |  |  |  |  |

**Completed by:** Data Protection Officer

Name ………………………………………………………….. Signature ……………………………………………… Date………………………………

**Approved by:** Senior Information Risk Owner

Name ………………………………………………………….. Signature ……………………………………………… Date………………………………

**Integrate the PIA outcomes back into the project plan**

***NB. This must include any actions identified in Table 1 and Table 2.***

|  |
| --- |
| **Who is responsible for integrating the PIA outcomes back in to the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns which may arise in the future?** |
| **Ref No.** | **Action to be taken** | **Date for completion of actions** | **Anticipated risk score following mitigation** | **Responsibility for action – *job title not names*** | **Current status/progress** |
| **Likelihood** | **Impact** | **RAG status** |
| *PR1* | *Communications plan to be developed* |  | *2* | *2* | *G* | *Project Manager to liaise with Communication lead and embed into project plan* | *Meeting arranged with Communication Lead* |
|  |  |  |  |  |  |  |  |

**Completed by:** Project Lead

Name ………………………………………………………….. Signature ……………………………………………… Date………………………………

# Appendix 1 Types of privacy risk

In all cases, guidance must be sought from the organisations risk management policy.

**Risks to individuals**

* Inadequate disclosure controls increase the likelihood of information being shared inappropriately.
* The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people’s knowledge.
* New surveillance methods may be an unjustified intrusion on their privacy.
* Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
* The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.
* Identifiers might be collected and linked which prevent people from using a service anonymously.
* Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.
* Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised.
* Information which is collected and stored unnecessarily or is not properly managed so that duplicate records are created, presents a greater security risk.
* If a retention period is not established information might be used for longer than necessary.

**Compliance risk**

* Non-compliance with the common law duty of confidentiality
* Non-compliance with the duties in the Health & Social Care (Safety & Quality) Act 2015
* Non-compliance with the DPA/GDPR.
* Non-compliance with the Privacy and Electronic Communications Regulations (PECR).
* Non-compliance with sector specific legislation or standards.
* Non-compliance with human rights legislation.

**Associated organisation/corporate risk**

* Non-compliance with the DPA/GDPR or other legislation can lead to sanctions, fines and reputational damage.
* Problems which are only identified after the project has launched are more likely to require expensive fixes.
* The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organisation.
* Information which is collected and stored unnecessarily or is not properly managed so that duplicate records are created, is less useful to the business.
* Public distrust about how information is used can damage an organisation’s reputation and lead to loss of business.
* Data losses which damage individuals could lead to claims for compensation.

# Guidance for completing a risk register

* What is the actual risk? Make sure the risk is clear and concise and articulated with appropriate use of language, suitable for the public domain.
* Be careful and sensitive about the wording of the risk as risk registers are subject to the Freedom of Information (FOI) requests
* Don’t reference blame to other organisations in the risk register (the register may be made available in the public domain)
* Does the risk belong to a business area within your organisation or another body?

It is common to use a RAG matrix rating system for assessing risk. RAG stands for red, amber, green. To achieve a RAG rating, each risk first needs a likelihood and impact score. Each risk will be RAG rated by taking the likelihood and impact scores, and using the matrix below:

|  |  |
| --- | --- |
| **Likelihood** | **Score** |
| **Likelihood** | **1** | **2** | **3** | **4** | **5** |
| **Descriptor** | **Rare** | **Unlikely** | **Possible** | **Likely** | **Almost Certain** |
| Frequency – how often might it happen? | This probably will never happen/recur | Do not expect it to happen/reoccur, but it is possible it may do so | Might happen or recur occasionally | Will probably happen/recur, but is not a persisting issue or circumstance | Almost certain to happen/recur; possibly frequently |

|  |  |
| --- | --- |
| **Impact** | **Score** |
| **Impact score** | **1** | **2** | **3** | **4** | **5** |
| **Descriptor** | **Very low** | **Low** | **Medium** | **High** | **Very high** |
| Impact should it happen | Unlikely to have any impact | May have an impact | Likely to have an impact | Highly probable it will have a significant impact | Will have a major impact |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Impact** | **Very High - 5** | **A** | **A/R** | **R** | **R** | **R** |
| **High – 4** | **A** | **A** | **A/R** | **R** | **R** |
| **Medium – 3** | **A/G** | **A** | **A** | **A/R** | **A/R** |
| **Low – 2** | **G** | **A/G** | **A/G** | **A** | **A** |
| **Very Low - 1** | **G** | **G** | **G** | **G** | **G** |
|  | **1 Rare** | **2 Unlikely** | **3 Possible** | **4 Likely** | **5 Almost Certain** |
| **Likelihood** |

Using the risk “RAG” rating system for scoring risks means risks can be ranked so that the most severe are addressed first.