Appendix 1a

West Midlands Pension Fund

GENERAL DATA PROTECTION REGULATIONS

PRIVACY IMPACT ASSESSMENT

This Privacy Impact Assessment must be completed wherever there is a change to an existing process or service, or a new process or information asset is introduced that is likely to involve a new use or significantly changes the way in which personal data is handled.

PIA Reference Number	
Project Description	
Implementing Service Area	
Project Manager details Name Designation Contact details	
Overview (Summary of the proposal and aim of project achievement)	
State the purpose of the project – e.g. operations, administration, research, audit etc.	
Key stakeholders (including contact details)	
Implementation date	

Appendix 1a

Stage 1 – Initial Screening Questions

Answering "Yes" to any of the screening questions below represents a potential IG risk factor that will have to be further analysed to ensure those risks are identified, assessed and fully mitigated.

Q	Category	Screening question	Yes/No
1.1	Identify	Will the project involve the collection of new information about individuals?	
1.2	Identify	Will the project compel individuals to provide information about themselves?	
1.3	Multiple organisations	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	
1.4	Data	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	
1.5	Data	Does the project involve using new technology which might be perceived as being privacy intruding for example biometrics or facial recognition?	
1.6	Data	Will the project result in you making decisions or taking action against individuals in ways which could have a significant impact on them?	
1.7	Data	Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example health records, criminal records, or other information that people are likely to consider as private?	
1.8	Data	Will the project require you to contact individuals in ways which they may find intrusive?	

If you have answered "Yes" to any of the questions below please proceed and complete stage 2.

Stage 2 – Privacy Impact Assessment

<table>
<tr><td>2.1</td><td>Is this a new or changed use of personal information that is already collected?</td><td colspan="3">New/Changed</td></tr>
<tr><td>2.2</td><td colspan="4">What data will be collected?
Administration data
Forename: ☐
Surname: ☐
DOB: ☐
Pension Reference: ☐
Address: ☐
NINO: ☐

Another unique identifier (please specify):
Other data (please state):

Sensitive data
Racial or ethnic origin: ☐
Political opinion: ☐
Religious belief: ☐
Trade union membership: ☐
Physical or mental health or condition: ☐
Sexual life: ☐
Commission or alleged commission of an offence: ☐
Proceedings for any offence committed or alleged: ☐
Biometric data ☐

Will the dataset include financial data? Yes/No

Description of other data collected

Is this information being used for a different purpose than it was originally collected for?</td></tr>
<tr><td rowspan="6">2.3</td><td colspan="2">Are other organisations involved in processing the data?</td><td colspan="2">Yes/No
If yes, list below</td></tr>
<tr><td colspan="2">Where “yes”, has the organisation signed a Data Sharing Agreement</td><td colspan="2"></td></tr>
<tr><td>Name and contact details</td><td>Data Controller (DC) or Data Processor (DP)?</td><td colspan="2">Completed and compliant with the IG Toolkit</td></tr>
<tr><td></td><td></td><td>Complete – Y/N</td><td>Overall rating</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td>2.4</td><td colspan="2">Has a data flow mapping exercise been undertaken?
If yes, please provide a copy – template attached, if no, please undertake.</td><td colspan="2">Yes/No</td></tr>
<tr><td>2.5</td><td colspan="2">Does the work involve employing contractors external to the organisation?</td><td colspan="2">Yes/No</td></tr>
</table>

	If yes, provide a copy of the confidentiality agreement or contract?	
2.6	Describe in as much detail why this information is being collected/used?	
2.7	Will the information be collected electronically, on paper or both?	Electronic: ☐ Paper: ☐
2.8	Where will the information be stored?	
2.9	Will this information be shared outside the organisations listed above in question 3? *If yes, describe who and why:*	
2.10	Is there an ability to audit access to the information?	Yes/No
2.11	Does the system involve new links to personal data held in other systems or have existing links been significantly changed?	
2.12	How will the information be kept up to date and checked for accuracy and completeness (data quality)?	
2.13	Who will have access to the information? (list individuals or staff groups)	
2.14	What security and audit measures have been implemented to secure access to and limit use of personal identifiable information? Username and password: ☐ Keys to locked cabinets: ☐ Restricted access to network files: ☐ Door access cards: ☐ Other (provide description):	
2.15	Will any information be sent offsite – i.e. outside the organisation and its computer network? And, are you transferring personal data to a country or territory outside of the EEA?	
2.16	Please state by which method the information will be transferred? Email (internal): ☐ Email (external): ☐ Website access: ☐ Post (internal): ☐	

	Post (external): ☐ Telephone: ☐ Fax: ☐ Courier: ☐ By hand: ☐ Wireless network: ☐ Other (please specify):		
2.17	Are disaster recovery and contingency plans in place?	Yes/No	
2.18	Is mandatory staff training in place for the following? • Data collection • Use of the system or service • Collecting consent • Information Governance	Yes/No Yes/No Yes/No Yes/No	Dates
2.19	Are there any new or additional reporting requirements for this project? • Who will be able to run reports? • Who will receive the report or where will it be published? • Will the reports be in person-identifiable, pseudonymised or anonymised format?	Yes/No	
2.20	If this new/revised function should stop, are there plans in place for how the information will be retained/archived/transferred or disposed of?	Yes/No	
2.21	How will individuals be informed about the proposed uses of their personal data? (e.g. privacy notices)		
2.22	Are arrangements in place for recognising and responding to members requests for access to their personal data?	Yes/No	
2.23	Will members be asked for their consent for their information to be collected and/or shared? *If no, list the reason for not gaining consent, e.g. relying on an existing agreement, consent is implied or other.* *How will you manage the member/service user dissent?*	Yes/No	

Appendix 1a

Data Mapping

Data mapping should be completed for each 'point of rest' of data being numbered from 1 onwards. 'Data at rest' includes electronic information in a system, spreadsheet or database or on paper in a filing system etc.

For each point of 'data at rest' answer the following questions in the corresponding section number:

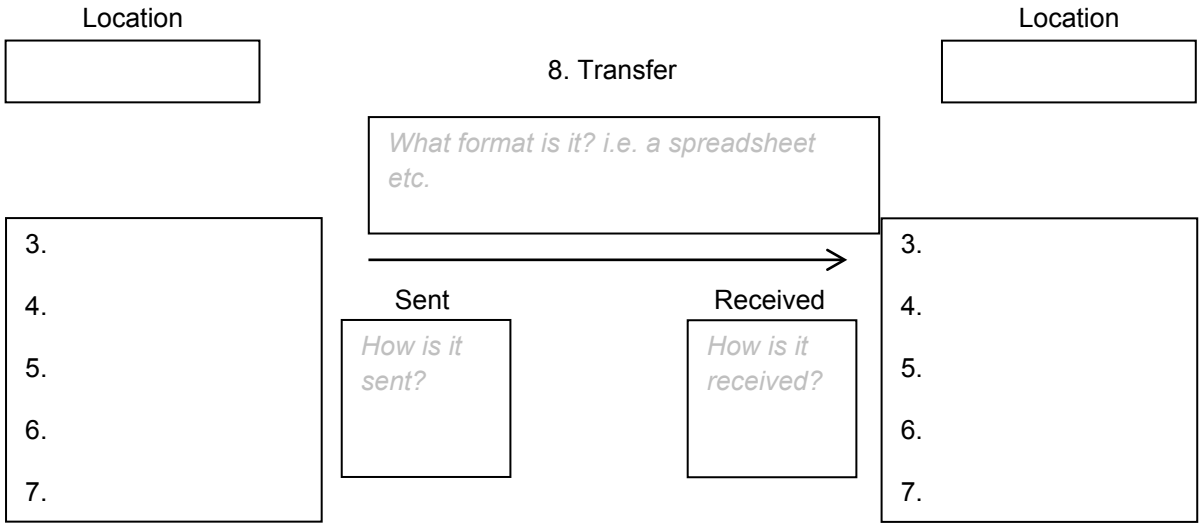
Q	Question	Section for completion
1	What data fields are included e.g. first name, last name, date of birth, postcode, diagnosis etc?	Data Fields Table (3.1)
2	How has the data been gathered? Eg extract from existing system, questionnaire, consolidation etc.	Data Fields Table (3.1)
3	Who has access to the data and what is the process for gaining access?	Data Mapping (3.2)
4	Is there an audit trail showing each time the data is accessed and by whom?	Data Mapping (3.2)
5	What is the format of the data at this point and how is it stored? E.g. paper, electronic, safe haven, encryption, security etc.	Data Mapping (3.2)
6	Who is responsible for the data at this point?	Data Mapping (3.2)
7	Is the data to be shared? If so with who? E.g. will it be shared with other organisations such as LGA, employer, AVC provider etc?	Data Mapping (3.2)
8	Please indicate how data is moved between the points of rest i.e. if electronically is it over a secure route such as local area network, internal email etc.	Data Mapping (3.2)

3.1 – Data Fields Table

Box number (Data flow mapping exercise)	Name of field	What is the source of the data? Which system is it from?	Justification for use

Appendix 1a

3.2 – Data mapping



Appendix 1a

PRIVACY IMPACT ASSESSMENT – Assessment of Legal Compliance

(To be completed by the Data Protection Officer)

PIA Reference No……..

Does the PIA meet the requirements under the Data Protection Act?

Principle No	Principle detail	Section reference	Assessment of Compliance
1	Personal data shall be processed fairly and lawfully fairly and in a transparent manner in relation to individuals	2.21 2.23	
2	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purpose	2.2	
3	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed	2.1	
4	Personal data shall be 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.	2.12	
5	Personal data must be kept in a form which permits identification of data subjects for no longer than 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 interests, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by GDPR in order to safeguard the rights and freedoms of individuals	2.12 2.20	
6	Personal data shall be 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 meansures	2.22 2.23	

Common Law Duty of Confidentiality

	Assessment of Compliance
Has the individual to whom the information relates given consent?	

Is the disclosure in the overriding public interest?	
Is there a legal duty to do so, for example a court order?	
Is there a statutory basis that permits disclosure? i.e. government	

Human Rights Act 1998

The Human Rights Act establishes the right to respect for private and family life. Current understanding is that compliance with the Data Protection Act and the common law of confidentiality should satisfy Human Rights requirements.

Will your actions interfere with the right to privacy under Article 8 of the Human Rights Act?	Yes/No
Have you identified the social need and aims of the project?	Yes/No
Are your actions a proportionate response to the social need?	Yes/No

Appendix 1a

Stage 3 – Privacy Impact Assessment

Producing a PIA report

In most small scale projects the PIA may identify one or more IG risks and the lead manager will be advised on the actions necessary to mitigate or eliminate those risks.

Where the PIA discovers complex or several IG risks, the IG Lead will conduct a further more detailed assessment (a full scale PIA) and produce a report.

The final report should cover (where applicable):

- A description of the proposal including the data flow process
- The case justifying the need to process an individual's personal data and why the particular policy or project is important
- An analysis of the data protection issues arising from the project
- Details of the parties involved
- Details of the issues and concerns raised
- Discussions of any alternatives considered to meet those concerns, the consultation process, and the rationale for the decisions made
- A description of the privacy by design features adopted
- An analysis of the public interest of the scheme
- Compliance with the data protection principles
- Compliance with the Government Data Handling review's information security recommendations
- Where the proposal involves the transfer and storage of personal data the PIA should include details of any security measures that will be put into place to ensure the data is protected and kept secure.

Appendix 1a

Authorisation records and action plan

Identifiable risks, agreed action plan and authorisation form

What are the key privacy issues and associated compliance and corporate risks? (Some Privacy Issues may have more than one type of risk i.e. it may be a risk to individuals and a corporate risk)

Privacy issue	Risk to individuals	Compliance risk	Corporate risk

What actions could you take to reduce the risk and note any further steps that may be necessary (e.g. new guidance notes)

Risk	Solution/s	Conclusion – is the risk reduced, eliminated or accepted?

What solutions need to be implemented?

Risk	Approved solution	Solution approved by

Actions

Action to be taken	Date for completion	Responsibility for action

Appendix 1a

Sign off

Data Protection Officer	
Name	
Job Title	
Signature	
Date	

Lead/Project Manager	
Name	
Job Title	
Signature	
Date	

Appendix 1a

What are the grounds for processing personal/personal sensitive data?

General Data Protection Regulations

Lawfulness of Processing – Article 6

Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(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;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

Conditions for Consent – Article 7

Consent under the GDPR must be a freely given, specific, informed and unambiguous indication of the individual's wishes. There must be some form of clear affirmative action – or in other words, a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity. Consent must also be separate from other terms and conditions, and you will need to provide simple ways for people to withdraw consent.

1.Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

2.If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

3.The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

4.When assessing whether consent is freely given, utmost account shall be taken of whether, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

What is the legitimate interest's condition?

The General Data Protection Regulations recognise that you may have legitimate reasons for processing personal data that the other conditions for processing do not specifically deal with. The "legitimate interests" condition is intended to permit such processing, provided you meet certain requirements.

The first requirement is that you must need to process the information for the purposes of your legitimate interests or for those of a third party to whom you disclose it.

The second requirement, once the first has been established, is that these interests must be balanced against the interests of the individual(s) concerned. The "legitimate interests" condition will not be met if the processing is unwarranted because of its prejudicial effect on the rights and freedoms, or legitimate interests, of the individual. Your legitimate interests do not need to be in harmony with those of the individual for the condition to be met. However, where there is a serious mismatch between competing interests, the individual's legitimate interests will come first.

Finally, the processing of information under the legitimate interests condition must be fair and lawful and must comply with all the data protection principles.

What Conditions need to be met in respect of special categories of personal data? Article 9

1.Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2.Paragraph 1 shall not apply if one of the following applies:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
(e) processing relates to personal data which are manifestly made public by the data subject;
(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
(i) processing is 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 quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; 4.5.2016 L 119/38 Official Journal of the European Union EN
(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

3.Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

4.Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

Appendix 1a

Common Law Duty of Confidentiality

The general position is that, if information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the data subject's consent.

The four sets of circumstances that make disclosure of confidential information lawful are:

- where the individual to whom the information relates has given consent;
- where disclosure is in the overriding public interest;
- where there is a legal duty to do so, for example a court order; and
- where there is a statutory basis that permits disclosure such as Local Government regulations

Therefore, under common law, a pension provider wishing to disclose a member's personal information to anyone outside the Fund should first seek the consent of that member. Where this is not possible, an organisation may be able to rely on disclosure being in the overriding public interest. However, whether a disclosure is in the public interest is not a decision to be taken lightly. The judgement to be made needs to balance the public interest in disclosure with both the rights of the individual(s) concerned and the public interest in maintaining trust in a confidential service. Solid justification is therefore required to breach confidentiality and any decision to disclose should be fully documented.

References

Privacy Impact Assessments – The Information Commissioners Office
http://www.ico.gov.uk/for_organisations/topic_specific_guides/pia_handbook.aspx.

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN