Annex 2: Information sharing arrangements

1. In this Memorandum of Understanding (MoU) **"Data Protection Legislation", "data subject(s)"**, **"personal data"**, **"process"**, **"processed"**, and **"processing"** shall have the meanings set out in, and will be interpreted in accordance with the General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA).

2. To the extent that the information being shared is personal data ("shared personal data"), both organisations agree to process it in compliance with all applicable laws, enactments, regulations, orders, standards and other similar instruments that apply to personal data processing (including but not limited to the requirements of Data Protection Legislation).

3. Each organisation undertakes that it:

   i. Will process any shared personal data fairly and lawfully and has legitimate grounds under the Data Protection Legislation.

   ii. Is entitled to provide the shared personal data and will ensure that the personal data is accurate.

   iii. Will respond within a reasonable time and as far as reasonably possible to enquiries from the Information Commissioner's Office (ICO) in relation to the shared personal data.

   iv. Will respond to subject access requests in accordance with the Data Protection Legislation.

   v. Will not disclose or transfer the shared personal data to a third party controller located outside the EEA unless it:

      a) Complies with the provisions of Articles 26 of the GDPR (in the event the third party is a joint controller); and

      b) Ensures that (i) the transfer is to a country approved by the European Commission as providing adequate protection pursuant to Article 45 of the GDPR; (ii) there are appropriate safeguards in place pursuant to Article 46 of the GDPR; or (iii) one of the derogations for specific situations in Article 49 of the GDPR applies to the transfer.

   vi. Will take all appropriate steps to have in place appropriate technical and organisational security measures to:

      a) prevent unauthorised or unlawful processing of the shared personal data;

b) prevent the accidental loss or destruction of, or damage to, the shared personal data;

c) ensure a level of security appropriate to the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage; and the nature of the shared personal data to be protected;

d) ensure that its staff members are appropriately trained to handle and process the shared personal data in accordance with the technical and organisational security measures together with any other applicable national data protection laws and guidance and have entered into confidentiality agreements relating to the processing of personal data.

vii. Each organisation will be responsible for ensuring that appropriate data security controls are in place appropriate to the nature and sensitivity of the material and its source, and their respective protective markings. These will include:

a) restricting access to the data to staff members on a 'need to know' only basis;

b) carrying out duties in accordance with statutory powers and responsibilities;

c) keeping information securely when not being accessed by these members of staff;

d) storing data on a system with security controls that ensures only access is by necessary and relevant people.

4. The organisations shall each comply with its obligation to report a personal data breach to the ICO and (where applicable) data subjects under Article 33 of the GDPR and shall each inform the other organisation of any personal data breach relating to the shared personal data under this MoU, irrespective of whether there is a requirement to notify the ICO or data subject(s).

5. The organisations agree to provide reasonable assistance as is necessary to each other to facilitate the handling of any personal data breach in an expeditious and compliant manner.