Memorandum of Understanding

Between

The Scottish Parliamentary Corporate Body

And

The Scottish Information Commissioner

This Memorandum of Understanding (MoU) is drawn up to provide the conditions on which the Scottish Parliamentary Corporate Body (SPCB) agrees to share the services of its designated data protection officer (DPO) with the Scottish Information Commissioner (the Commissioner) in accordance with the requirements of the General Data Protection Regulation (GDPR) that comes into effect on 25 May 2018 and the Data Protection Act 2018 (DPA 2018) which is due to come into force in May 2018

This MOU does not affect the obligations placed on the Commissioner as a data controller, for his or her compliance with the GDPR or the DPA 2018.

1. Background

The GDPR and the DPA 2018 provide a modernised, accountability-based compliance framework for data protection. Data Protection Officers (DPOs) will be central to the new legal framework for facilitating compliance with the provisions of the legislation.

Under the GDPR, it is mandatory for public authorities to designate a DPO.

Article 37(3) of the GDPR allows several public bodies to designate a single DPO taking account of their organisational structure and size.

Similarly, Part 3 of the DPA 2018 allows the same person to be designated as a DPO by several controllers.

Annex A sets out the tasks of the DPO as provided for in Article 39 of the GDPR.

2. Shared Services

Under the Shared Services Agenda for parliamentary officeholders, the SPCB intends to share the services of its DPO with the parliamentary office holders.

3. Conditions

The DPO will act as the Commissioner's designated DPO, on the following conditions:-

3.1 The Commissioner will observe the conditions relating to the position of the DPO in Article 38.1, 2 and 3 of the GDPR at all times.

3.2 The DPO will perform the tasks set out in Article 39 of the GDPR, in accordance with Annex A.

3.3 The services of the DPO are provided without charge to the Commissioner but the Commissioner will, along with the other parliamentary officeholders, be financially responsible for any bespoke training they require that is not provided centrally by the SPCB.

3.4 Recognising that this is a shared service, the Commissioner accepts that the DPO's services are provided according to need.

3.5 The Commissioner will be expected to utilise the DPO's time efficiently and to consider alternative arrangements such as enabling the DPO to participate in relevant meetings remotely.

3.6 For the purposes of section 45 of the Freedom of Information Scotland Act 2002 (FOISA) and regulation 18(5) of the Environmental Information (Scotland) Regulations 2004, (the EIRs) the DPO is an agent of the Commissioner.

3.7 In the event of a potential, suspected or actual data breach, the DPO will assist the Commissioner's staff in an advisory capacity by providing guidance on identifying whether a breach has taken place and recommend actions to take.

3.8 When the DPO is acting for the Commissioner in an advisory capacity, neither the DPO, nor the SPCB in any circumstances, will be liable for any non-compliance with the GDPR or DPA 2018 by the Commissioner.

4. Confidentiality

4.1 The Commissioner has specific duties under section 45 of FOISA and the EIRs about maintaining confidentiality, and must ensure that the organisation maintains its independence and impartiality, and avoids conflicts of interest.

4.2 Section 45 of FOISA and regulation 18(5) of the EIRs also apply to the DPO as an agent of the Commissioner. In this context, all information received by the DPO from the Commissioner for the purposes of delivering the DPO services shall be kept confidential and will not be disclosed to any third party without the consent of the Commissioner, unless required to be disclosed by law or judicial decree. Third-party is understood to mean any person external to the office of the Commissioner. However, the obligation of secrecy/confidentiality does not prohibit the DPO from contacting and seeking advice from the ICO.

4.3 The DPO will undertake to return any information and/or personal data provided by the Commissioner within an agreed timeframe.

5 Conflicts of interest

5.1 It is not anticipated that conflicts of interest are likely to arise. However, should any conflict of interest occur, or a situation arise in which the DPO considers that a conflict of interest is likely to occur, the DPO should immediately notify the Commissioner and will cease to provide DPO services to the Commissioner in relation to that specific conflict of interest.

5.2 The Commissioner will, in such a situation, use alternative DPO services.

6 Complaints and Dispute resolution

6.1 The Commissioner, the SPCB and the DPO shall attempt in good faith to negotiate a settlement to any dispute between them arising out of or in connection with this MOU within 20 working days of either party notifying the other in writing of the dispute.

6.2 The escalation process for any dispute will be:

- As regards complaints raised by the Commissioner: the Group Head of Digital Services Group will review and respond to complaints raised by the Commissioner's Business Manager;
- Where a dispute is unresolved, the Commissioner may escalate the complaint to an Assistant Chief Executive who shall investigate and respond within 20 working days;
- As regards complaints by the DPO: the Commissioner will investigate and respond within 20 working days

7 Review mechanism

7.1 The services outlined in and operation of this MoU will be reviewed one year after its commencement. The parties will meet to consider where the MoU worked well and identify any issues. The aim of the review is to resolve any issues and embed good practice. If required, the MoU will be amended. If the parties cannot agree, the dispute resolution process will come into effect. After the initial review, either party may request a review of the MoU as and when required.

8 Termination

8.1 Either party may terminate this agreement on giving 60 working days' notice in writing. The dispute resolution process must be exhausted prior to a termination notice being issued.

Signed…… Date……
Scottish Information Commissioner

Signed……. Date…….
For the SPCB

Signed……. Date……
Data Protection Officer

A1. The data protection officer shall have at least the following tasks:

A1.1 to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to the GDPR and to other Union or Member State data protection provisions;

A1.2 to monitor compliance with the GDPR, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

A1.3 to provide advice where requested as regards a data protection impact assessment (DPIA) and monitor its performance pursuant to Article 35;

A1.4 to cooperate with the supervisory authority;

A1.5 to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

A1.6 The DPO shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

A2. Commissioner's requirements of the DPO

The DPO will:-

A2.1 attend, in an advisory capacity, senior management meetings where decisions with data protection implications are taken;

A2.2 attend, by invitation, such other meetings/working groups dealing with data processing activities;

A2.3 provide advice to the Commissioner on matters relating to data protection; provide advice to the Commissioner where requested as regards the DPIA requirements in Article 35 of the GDPR and Chapter 4 of Part 3 of the DPA 2018 and monitor his or her performance including (i) whether or not to carry out a DPIA; (ii) what methodology to follow when carrying out a DPIA; (iii) whether to carry out the DPIA in-house or whether to outsource it; (iv) what safeguards (including technical and organisational measures) to apply to mitigate any risks to the rights and interests of the data subjects; (v) whether or not the DPIA has been correctly carried out and (vi) whether its conclusions (whether or not to go ahead with the processing and what safeguards to apply) are in compliance with the GDPR and/or the DPA 2018;

A2.4 inform and advise the Commissioner and his employees about their obligations under the GDPR, the DPA 2018 and any other data protection laws;

A2.5 assist the Commissioner to identify if a data breach has occurred or where a data breach or incident has occurred. The timescales for providing assistance are set out in paragraph A4 below;

A2.6 co-operate with the ICO and act as a contact point for the ICO on issues relating to processing, and to consult, where appropriate, with regard to any other relevant matter;

A2.7 act as a contact point to facilitate access by the ICO to the documents and information for the performance of the tasks, as well as for the exercise of its investigative, corrective, authorisation and advisory powers; and

A2.8 be accessible and available to communicate (efficiently and clearly) with data subjects in relation to their rights.

A3. Compliance

The DPO will assist the Commissioner to monitor compliance by:-

A3.1 informing themselves fully of how the Commissioner processes data;

A3.2 advising on DPIAs and Privacy Impact Assessments (PIAs);

A3.3 conducting internal audits;

A3.4 providing an annual assurance report;

A3.5 collecting information to identify processing activities;

A3.6 awareness-raising, through training of employees involved in the processing operations, and the related audits;

A3.7 providing advice where required as regards DPIAs and monitoring the Commissioner's performance in line with Article 35 of the GDPR/Chapter 4 of Part 3 of the DPA 2018;

A3.8 co-operating with the ICO;

A3.9 analysing and checking compliance of processing activities;

A3.10 informing, advising and issuing recommendations to the data controller and processor;

A3.11 acting as the contact point for the ICO on issues relating to the processing of personal data;

A3.12 informing, advising and issuing recommendations to the data controller and processor; and

A3.13 being available to employees of the Commissioner and data subjects.

A4. Accessibility

A4.1 The DPO and her team can be contacted as follows:-

Named DPO Claire Turnbull	Tel (office hours): 0131 348 6080 Email: DPOservice@parliament.scot
DPO Team	Tel (office hours): 0131 348 6080 Email: DPOservice@parliament.scot
Office Hours	Mon-Thurs: 8.30am to 5pm

	Friday: 8.30am to 4.30pm
Out of Hours	Mon-Fri (8am to 6pm) - 0131 348 6100 During Recess (Mon-Fri) 8.30am to 5pm - 0131 348 6100 Voicemail service at all other times - 0131 348 6100

A4.2 The DPO and her team will be accessible to the Commissioner as follows:-

Activity	Contact options	Timescale
Attending senior management meetings where data protection issues are being discussed. The DPO will attend for data protection agenda items only.		As timetabled
Providing advice on data protection issues	Telephone or email	On receipt of all relevant information:- Non urgent – within 5 working days or as agreed Urgent – within 24 hours of initial contact with the DPO Team
<u>Training</u> The Commissioner may request training for his staff The DPO may identify training needs.	Requests for training should be made via the DPO Team The DPO will notify the Commissioner and the other officeholders of training opportunities	As agreed
Assisting the Commissioner to determine if there has been a breach	Telephone, conference call or email	Within 24 hours
Attend such other meetings/working groups dealing with data protection activities	Requests for DPO to attend meetings etc should be made via the DPO Team	Such reasonable notice as is necessary

A4.3 Where the DPO is temporarily unavailable due to illness or other cause, or during the normal period of annual leave, her/his duties will be assigned to a named member of the DPO Team.

A4.4 If the DPO's post is vacant, her/his duties will be assigned to a named member of the DPO Team.

A5. <u>Role of Commissioner</u>

The Commissioner will:-

A5.1 publish contact details of the DPO

A5.2 communicate the contact details of the DPO to the ICO

A5.3 promptly consult with the DPO when an incident concerning the processing of personal data has occurred

A5.4 maintain a record of processing operations under his responsibility;

A5.5 provide the DPO with sufficient information to enable the DPO to accurately relay information to the ICO on how they process personal data. This will ideally be in the form of a flowchart.

A5.6 provide the DPO with contact details for his/her office, including out of hours contact details

A5.7 liaise with the DPO to timetable routine meetings and training sessions giving the DPO at least 4 weeks advance notice

A5.8 as regards other meetings give the DPO as reasonable advance notice as possible.

A5.9 co-operate with the DPO and his/her team

A5.10 invite the DPO to attend meetings where decisions with data protection implications are taken. All relevant information must be passed on to the DPO in a timely manner in order to allow him or her to provide adequate advice;

A5.11 shall seek the DPO's advice when carrying out a DPIA or PIA;

A5.12 if he/she so chooses, develop data protection guidelines or programmes that set out when the DPO must be consulted