Contents

1. Introduction 3
2. Policy statement 4
3. What personal information is covered? 5
4. Principles 5
5. Information Collection 7
   5.1 Collecting personal information 7
   5.2 Data Subject Consent 8
   5.3 Data Subject Notification 9
   5.4 External Privacy Notices 10
   5.5 Information Use 10
   5.6 Information Quality 12
   5.7 Information Retention 12
6. Data Subject Requests 13
7. Responsibilities under this policy 13
   7.1 Overall responsibilities 13
   7.2 Data Protection Reviewer (DPR) responsibilities 14
   7.3 Line managers’ responsibilities 14
   7.4 General responsibilities 15
8. Information Protection by Design 15
9. Monitoring and audits 16
10. What to Do If There Is a Breach 17
11. Validity of this policy 17

Appendix A Eight Principles of Data Protection 18
Appendix B Legitimate Interests Assessment Form 21
Appendix C Data Protection Subject Access Request Form 23
Appendix D Data Protection Impact Assessment Template 28
1. **Introduction**

1.1 The Commonwealth Parliamentary Association (**CPA**) needs to collect personal information about individuals in order to carry out its functions and fulfil its objectives.

1.2 Irrespective of how information is collected, recorded and otherwise processed personal information must be dealt with properly to ensure compliance with the Data Protection Act (DPA) 1988 which is replaced on 25th May 2018 by General Information Protection Regulations (GDPR) 2016.

1.3 The lawful and correct treatment of personal information by CPA is paramount to the success of the organisation and to maintaining the confidence of its members, partners and employees. Getting it wrong is serious for the CPA and could lead to complaints from individuals, compensation claims, fines from regulators and negative publicity.

1.4 The policy will be reviewed annually by the CPA, to reflect both changes in the law and in CPA policy and practice.
2. **Policy statement**

2.1 This document defines the GDPR policy and practice for the CPA. It applies to all personal information obtained and processed by the organisation and its employees. It sets out:

- the organisation’s policy for the protection of all personal information that is processed
- establishes the responsibilities (and best practice) for information protection
- references the key principles of the Data Protection Act 1998 and GDPR.

2.2 This policy applies to all Processing of Personal Information in electronic form (including electronic mail and documents created with word processing software) or where it is held in manual files that are structured in a way that allows ready access to information about individuals.

2.3 This policy will ensure that personal information is processed, handled, transferred, disclosed and disposed of lawfully. Personal information should be handled in the most secure manner by authorised staff only, on a need to know basis.

2.4 The policy covers all personal information whether a member or non-member of the CPA, electronic or paper which may relate to members, participants, employees, contractors and third parties about whom we hold information.

2.5 For the purposes of this policy the following definitions are relied upon:

*Processing of information*: how information is collected, held, accessed, transferred and managed

*Data Subject*: used to denote an individual about whom data/information is held.

*Data Controller*: used to denote the entity with overall responsibility for data collection and management. The CPA is the Data Controller for the purposes of the Act.

*Data Processor*: an individual handling or processing data

*Personal information*: any information which enables a person to be identified

*Special categories of personal data* information under the Regulations which requires explicit consent for it to be held by the CPA

---

1. **Article 9(1) GDPR** sets out the special categories of personal data:

"... 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..."
3. **What personal information is covered?**

3.1 Personal information within the respective legislative and regulatory provisions covers ‘any information that can be used to identify a living individual either directly or indirectly’. Individuals can be identified by various means including but not limited to, their address, telephone number or e-mail address. Anonymised or aggregated information is not regulated by the provisions, providing the anonymization or aggregation of the information is irreversible.

3.2 Personal information (or personal data) is defined as ‘any information relating to an identified or identifiable natural person’ an ‘identifiable natural person’ being one who can be identified either directly or indirectly.

3.3 Personal information controlled by CPA can include that of employees (present, past and prospective), members, non-members, contractors and third parties, private and confidential information as well as sensitive information, whether in paper, electronic or other form.

3.4 The CPA obtains and processes personal information for a variety of different purposes, including but not limited to:

- staff records and administrative records;
- matters relating to the CPA’s legitimate business activities in Parliamentary Democracy and Strengthening of the in the development, planning and delivery of activities from outreach and communications to bespoke member programmes;
- complaints and requests for information

4. **Principles**

4.1 Data Protection legislation places a responsibility on every data controller to process any personal information in accordance with the eight principles. (More detailed guidance on how to comply with these principles can be found by following the this link to the ICO’s website ([ico.org.uk](http://ico.org.uk))

4.2 In order to comply with its obligations, CPA undertakes to adhere to the following eight principles as set out in Schedule 1 of the Data Protection Act 1988:

1) Processing personal data/information fairly and lawfully.

2) Process the data for the specific and lawful purpose for which it collected that data and not further process the data in a manner incompatible with this purpose.

3) Ensure that the data is adequate, relevant and not excessive in relation to the purpose for which it is processed.

4) Keep personal information accurate and, where necessary, up to date.

5) Only keep personal data for as long as is necessary.
6) Process personal information in accordance with the rights of the data subject under the legislation.

7) Put appropriate technical and organisational measures in place against unauthorised or unlawful processing of personal information, and against accidental loss or destruction of information.

8) Ensure that no personal information is transferred to a country or a territory outside the European Economic Area (EEA) unless that country or territory ensures adequate level of protection for the rights and freedoms of information subjects in relation to the processing of personal information.

4.2.1 See Appendix A for a more detailed explanation of how the CPA will look to meet each of the eight principles, however at a glance, to meet the responsibilities the CPA will:

- Ensure any new or planned projects that involve Personal Information are preceded with a Data Privacy Impact Assessment.
- Ensure that access controls are limited to role relevance.
- Ensure any personal information is collected in a fair and lawful way.
- Gain explicit consent where required.
- Explain at the outset why information is being collected, what it will be used for and with whom it will be shared.
- Ensure that only the minimum amount of information needed is collected and used.
- Ensure the information used is up to date and accurate.
- Review the length of time information is held\(^2\)
- Ensure information is kept safely.
- Ensure the rights people have in relation to their personal information can be exercised.
- Dispose of information appropriate and without unnecessary delay.
- Ensure that anyone managing and handling personal information is trained to do so.
- Ensure that anyone wanting to make enquiries about handling personal information, whether a member of staff, volunteer or service user, knows what to do.
- Any disclosure of personal information will be in line with relevant legislation, and internal policies and procedures.

\(^2\) See CPA Data Retention Policy
Any sharing of information to third parties is covered by an information sharing agreement.

Take measures to ensure safe transfers of information outside of the EU/EEU where cross border sharing is necessary.

5. Information Collection

5.1 Collecting personal information

5.1.1 Personal information does not need to be collected only from the individual – the key principles for information collection are:

(a) How privacy information will be provided – i.e. transparency and privacy notices

(b) That the CPA have a lawful purpose for collecting it and, where necessary, the CPA will obtain consent.

5.1.2 Personal Information should be collected only from the data subject unless one of the following apply:

- The nature of the business purpose necessitates collection of the personal information from other persons or bodies.

- The collection must be carried out under emergency circumstances in order to protect the vital interests of the data subject or to prevent serious loss or injury to another person.

- If personal information is collected from someone other than the data subject, the data subject must be informed of the collection unless one of the following apply:
  a. The data subject has received the required information by other means.
  b. The information must remain confidential due to a professional secrecy obligation.
  c. A law expressly provides for the collection, processing or transfer of the personal Information.

5.1.3 Where it has been determined that notification to a data subject is required, notification should occur promptly, but in no case later than:

- One calendar month from the first collection or recording of the Personal Information

- At the time of first communication if used for communication with the Data subject

- At the time of disclosure if disclosed to another recipient.
In essence providing the privacy notice to ensure transparency, always applies. If collected directly e.g. at a road show, it should be given at the point of collection. If collected indirectly, within one month.

5.2 Data Subject Consent

5.2.1 The CPA will only obtain personal information only by lawful and fair means and, where appropriate with the knowledge and consent of the individual concerned.

5.2.2 The CPA will therefore only collect and use personal information where:

(i) It is relevant to its legitimate business purposes (e.g. a HR purpose or for contract management reasons), having completed and stored a legitimate interest test on all new or planned activities, as per Appendix B

(ii) We can rely on a lawful basis (or bases);

(iii) The purposes are identified in the information privacy notice provided to individuals, and

(iv) The collection and use is within the individual’s expectations.

5.2.3 Where a need exists to request and receive the consent of an individual prior to the collection, use or disclosure of their personal information, the CPA is committed to seeking such consent.

5.2.4 The following table illustrates examples of what and when consent for various CPA scenarios would meet the requirements of unambiguous and/or explicit consent.

<table>
<thead>
<tr>
<th>Form of Consent</th>
<th>Unambiguous?</th>
<th>Explicit?</th>
</tr>
</thead>
<tbody>
<tr>
<td>A contract with the CPA includes a written declaration of the CPA’s/Customers consent to specified types of processing (the request being clearly distinguishable from other matters in the contract)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>The CPA website offers members the opportunity to opt-in to specified processing through a tick-box when ordering or subscribing for CPA materials</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

3 GDPR Definition of Consent: “Any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed”.
<table>
<thead>
<tr>
<th>Form of Consent</th>
<th>Unambiguous?</th>
<th>Explicit?</th>
</tr>
</thead>
<tbody>
<tr>
<td>At a CPA programme of event sign-in, participants are informed that the CPA and/or CPA event partners, would like to use their registration details for specified types of promotion/publicity/Monitoring and Evaluation are asked (verbally) whether they consent to such processing</td>
<td>Yes, consent may be given verbally, however staff must consider, per event, how consent will be documented with greater certainty given the GDPR accountability requirement.</td>
<td>No, whilst consent may be inferred from the actions of members/staff actions, it cannot be said to be explicit.</td>
</tr>
<tr>
<td>At ExCO, members and staff are informed that photographs will be being taken in a section of the building during a particular time and that such photos’ will be included on the CPA website and/or reports. Members/staff having been informed, go to the area in which photographs are being taken.</td>
<td>Yes, consent may be inferred from the members/employees actions in going to the area of the building in which photographs are being taken</td>
<td>No, whilst consent may be inferred from the actions of members/staff actions, it cannot be said to be explicit.</td>
</tr>
</tbody>
</table>

5.2.5 The Director of Operations, in cooperation with ‘Heads Of’, shall establish a system for obtaining and documenting Data subject consent (See Appendix C⁴), for the collection, processing, and/or transfer of their personal information. The system will include provisions for:

- Determining what disclosures should be made in order to obtain valid consent.
- Ensuring the request for consent is presented in a manner which is clearly distinguishable from any other matters, is made in an intelligible and easily accessible form, and uses clear and plain language.
- Ensuring the consent is freely given (i.e. is not based on a contract that is conditional to the processing of personal information that is unnecessary for the performance of that contract).
- Documenting the date, method and content of the disclosures made, as well as the validity, scope, and volition of the consents given.
- Providing a simple method for a data subject to withdraw their consent at any time.

5.3 Data Subject Notification

5.3.1 The CPA will provide data subjects with information as to the purpose of the Processing of their personal Information, by issuing a Privacy Notice and securing informed consent.

⁴ This relates to non-staff only. Information Subject Consents forms for staff are prepared separately.
5.3.2 When the data subject is asked to give consent to the processing of personal information and when any personal information is collected from the data subject, all appropriate disclosures will be made, in a manner that draws attention to them, unless one of the following apply:

- The Information Subject already has the information
- A legal exemption applies to the requirements for disclosure and/or Consent.

5.4 External Privacy Notices

5.4.1 The CPA external website includes an online ‘Privacy Notice’ however the CPA do not collect any personal identifiable data, such as IP addresses or email addresses, from the website.

5.4.2 This will remain under review and where the CPA Website is enabled to collect personal information on CPA activities the Privacy Notice will be updated and a link made available at the point of collection, fulfilling the requirements of GDPR.

5.5 Information Use

5.5.1 The CPA uses the Personal information of its Contacts for the following broad purposes:

- The general running and business administration of CPA Activities.
- To provide services to the CPA membership.
- The ongoing administration and management of member services.

5.5.2 The use of a member’s and/or partner/stakeholders contact information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object. For example, it would clearly be within a member’s expectations that their details will be used by CPA to respond to a request for information about CPA services on offer. However, it will not be within their reasonable expectations that the CPA would then provide their details to Third Parties for marketing purposes.

5.5.3 The CPA will only process personal information in accordance with all applicable laws and applicable contractual obligations. More specifically, the CPA will not process a member’s personal information unless at least one of the following requirements are met:

- The data subject has given consent to the processing of their personal information for one or more specific purposes.
- 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.
• Processing is necessary for compliance with a legal obligation to which the data controller is subject.

• Processing is necessary in order to protect the vital interests of the data subject or of another natural person.

• 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 data controller.

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

5.5.4 There are some circumstances in which personal information may be further processed for purposes that go beyond the original purpose for which the personal information was collected. When making a determination as to the compatibility of the new reason for processing, guidance and approval must be obtained from the Director of Operations/Data Protection Reviewer before any such processing may commence.

5.5.5 In any circumstance where consent has not been gained for the specific processing in question, the CPA will address the following additional conditions to determine the fairness and transparency of any processing beyond the original purpose for which the personal information was collected:

• Any link between the purpose for which the personal information was collected and the reasons for intended further processing.

• The context in which the personal information has been collected, in particular regarding the relationship between data subject and the data controller.

• The nature of the personal information, in particular whether special categories of information are being processed, or whether personal information related to criminal convictions and offences are being processed.

• The possible consequences of the intended further processing for the data subject. The existence of appropriate safeguards pertaining to further Processing, which may include Encryption, Anonymization or Pseudonymisation.

5.5.6 Staff should note however that consent does not override the requirement to keep information secure.
5.6 Information Quality

5.6.1 The CPA will adopt all necessary measures to ensure that the personal information it collects and processes is complete and accurate in the first instance, and is updated to reflect the current situation of the Information Subject.

5.6.2 The measures adopted by the CPA to ensure information quality include:

- Correcting personal information known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the Information Subject does not request rectification.

- Keeping personal information only for the period necessary to satisfy the permitted uses or applicable statutory retention period.

- The removal of Personal information if in violation of any of the Information Protection principles or if the Personal information is no longer required.

- Restriction, rather than deletion of personal information, insofar as:
  - A law prohibits erasure.
  - Erasure would impair legitimate interests of the data subject.
  - The data subject disputes that their personal information is correct and it cannot be clearly ascertained whether their information is correct or incorrect.

5.7 Information Retention

5.7.1 To ensure fair Processing, Personal information will not be retained by the CPA for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further Processed. (See CPA GDPR Retention Policy)

5.7.2 The length of time for which the CPA need to retain personal information is set out in the CPA’s GDPR Retention Policy. This takes into account the legal and contractual requirements, both minimum and maximum, that influence the retention periods set forth in the schedule.

All Personal information should be securely deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.
6. **Data Subject Requests**

6.1 Data subjects are entitled to obtain, based upon a request made in writing to the CPA Data Protection Reviewer – Director of Operations, see Appendix C, and upon successful verification of their identity.

6.2 If an individual makes a request relating to any of the rights listed below, the CPA will consider each such request in accordance with all applicable data protection laws and regulation. No administration fee will be charged for considering and/or complying with such a request unless the request is "manifestly" unnecessary or excessive in nature – this is likely to be in exceptional cases only and in most cases we will not charge any fee.

6.2.1 Where any Secretariat staff receive such a request, either verbally or writing, must inform the Data Protection Reviewer/Director of Operations

6.3 The Data Protection Reviewer/Director of Operations will facilitate the exercise of data subject rights related to:

- Information access.
- Objection to Processing.
- Objection to automated decision-making and profiling.
- Restriction of Processing.
- Information portability.
- Information rectification.
- Information erasure
- Withdrawing consent

6.4 It should be noted that situations may arise where providing the information requested by a data subject would disclose personal information about another individual. In such cases, information must be redacted or withheld as may be necessary or appropriate to protect that person’s rights.

7. **Responsibilities under this policy**

7.1 **Overall responsibilities**

7.1.1 The CPA, known as the ‘information controller’, permits the organisation’s staff to use computers and relevant filing systems (manual records) in connection with their duties. The CPA has a legal responsibility for the notification process and compliance of GDPR.

7.1.2 To demonstrate our commitment to Information Protection, and to enhance the effectiveness of our compliance efforts, CPA has appointed the Director of Operations, who has the necessary authority, as the Data Protection Reviewer (for the CPA).

7.1.3 All members of the Secretariat, including temporary and contract workers, who handles personal information for the CPA is responsible under the policy, and may be subject to disciplinary action if they do not follow it.
7.2  **Data Protection Reviewer (DPR) responsibilities**

7.2.1 The Information Protection Officers’ duties under GDPR includes:

- Informing and advising the CPA and staff, who carry out processing pursuant to Information Protection regulations, the relevant Data Protection provisions;

- Ensuring the alignment of this policy of Data Protection regulations with other Secretariat policies and practices;

- Providing guidance with regards to carrying out Data Protection Impact Assessments (DPIAs);

- Acting as a point of contact for and cooperating with Information Commissioners Office (ICO);

- Determining the need for notifications to the ICO as a result of the CPA’s current or intended Personal information processing activities;

- Making and keeping current notifications to the ICO as a result of the CPA’s current or intended Personal information processing activities;

- The establishment and operation of a system providing prompt and appropriate responses to Information Subject requests;

- Informing the Secretary-General, officers and staff of the CPA of any potential corporate, civil and criminal penalties which may be levied against the CPA and/or its Employees for violation of GDPR.

- Ensuring establishment of procedures and standard contractual provisions for obtaining compliance with this Policy by any Third Party who:
  - provides Personal information to the CPA;
  - receives Personal information from the CPA;
  - has access to Personal information collected or processed by a CPA partner, host or third party Entity.

7.3  **Line managers’ responsibilities**

7.3.1 All line managers across the CPA Secretariat are directly responsible for completing any privacy impact assessments for relevant work areas and to ensure staff:

- are made aware of this policy;

- are made aware of the results of the privacy impact assessment;
• are aware of their information protection responsibilities, including but not limited to issuing privacy notice(s) and securing and documenting informed consent;

• receive suitable information protection training.

7.4 General responsibilities

7.4.1 All CPA employees, including temporary and contract staff are subject to compliance with this policy. Under the GDPR individuals can be held personally liable for information protection breaches.

7.4.2 All CPA employees have a responsibility to inform their line manager and the Data Protection Reviewer (DPR) of any new use of personal information, as soon as reasonably practicable after it has been identified.

7.4.3 All CPA employees will, on receipt of a request from an individual for information held, known as a subject access request or concerns about the processing of personal information, immediately notify the DPR.

7.4.4 In addition, each staff will need to ensure all Third Parties engaged to process personal information on the CPA’s behalf (i.e. their Information Processors) are aware of and comply with the contents of this policy. Assurance of such compliance must be obtained from all Third Parties, whether companies or individuals, prior to granting them access to Personal information controlled by the CPA.

8. Information Protection by Design

8.1 To ensure that all Information Protection requirements are identified and addressed when designing new systems or processes and/or when reviewing or expanding existing systems or processes, each of them must go through an approval process before continuing.

8.2 For all CPA activities that involve personal information processing for new, and/or revised, systems or processes or programmes, a Data Protection Impact Assessment (DPIA) should be completed. (See Appendix D)

8.2.1 A Data Protection Impact Assessment (DPIA) is a process to help identify and minimise the data protection risks of a project.

8.2.2 Staff must do a DPIA for processing that is likely to result in a high risk to individuals. This includes some specified types of processing. The screening checklists at the beginning of the DPIA form will help you decide whether to complete a full DPIA.

8.2.3 It is also good practice to do a DPIA for any other major project which requires the processing of personal data.
8.2.4 The DPIA must:

- describe the nature, scope, context and purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

8.2.5 To assess the level of risk, staff must consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm.

8.2.6 Staff should consult the data protection reviewer and, where appropriate, individuals and relevant experts. Any processors may also need to assist you.

8.2.7 Having completed the DPIA if the Secretariat identify a high risk that cannot be mitigated, we must consult the ICO before starting the processing.

8.2.8 The ICO will give written advice within eight weeks, or 14 weeks in complex cases. If appropriate, they may issue a formal warning not to process the data, or ban the processing altogether.

ALL DPIA’S MUST RECORDED AND SAVED IN THE APPROPRIATE GDPR Y: DRIVE FOLDER FOR AUDIT PURPOSES

9. Monitoring and audits

9.1 Compliance with this policy will be monitored by the Director of Operations/ DPR, together with internal audit reviews where necessary.

9.2 To confirm that an adequate level of compliance is being achieved by all CPA activities in relation to this policy, the DPR will carry out an annual Data Protection compliance audit. Each audit will, as a minimum, assess compliance with this Policy in relation to the protection of personal information, which will include:

- The assignment of responsibilities.
- Raising awareness.
- Training of Employees.
- The effectiveness of Information Protection related operational practices, including:
  - Information Subject rights.
  - Personal Information transfers.
  - Personal Information incident management.
  - Personal Information complaints handling.
  - The level of understanding of Data Protection policies and Privacy Notices.
  - The currency of Information Protection policies and Privacy Notices.
  - The accuracy of Personal information being stored.
  - The conformity of Information Processor activities.
• The adequacy of procedures for redressing poor compliance and Personal information Breaches.

9.2.1 The DPR, in cooperation with key staff/stakeholders, will devise a plan with a schedule for correcting any identified deficiencies within a defined and reasonable time frame. Any major deficiencies identified will be reported to and monitored by the Executive Committee.

9.3 Training relating to responsibilities and awareness of GDPR for the CPA will include induction mandatory training and in house risk assessment and audits.

10. What to Do If There Is a Breach

10.1 If you discover, or suspect, a data protection breach you should report this to your line manager who will review our systems, in conjunction with the Head of IT, to prevent a reoccurrence.

10.2 The DPR should be informed of the breach, the action taken is recorded and outcomes to determine whether it needs to be reported to the Information Commissioner and also for reporting to the CPA Executive Committee.

10.3 The CPA will respond to any incident immediately which will includes a recovery plan and, where necessary, implement procedures for damage limitation.

10.3.1 The CPA will assess any risks associated with a breach, as these could affect any procedures after the breach has been contained. In particular, the CPA will assess:

• the potential adverse consequences for individuals;
• how serious or substantial these are;
• and how likely they are to re occur.

10.3.2 If appropriate the CPA will inform a data subject about an information security breach, the ICO; other regulatory bodies; other third parties such as the police and the banks; or the media.

10.3.3 There is a time limit for reporting breaches to ICO so the DPR should be informed without delay.

10.4 Any deliberate or reckless breach of this Data Protection Policy by an employee or volunteer may result in disciplinary action which may result in dismissal.

11. Validity of this policy

11.1 This policy will be reviewed at least annually under the authority of the CPA Secretary-General and will be subject to an ongoing development and review programme.
Appendix A – Eight Principles of Data Protection

1. Processing personal data/information fairly and lawfully.

The CPA will make all reasonable efforts to ensure that individuals who are the focus of the personal data (data subjects) are informed of the identity of the data controller, the purposes of the processing, any disclosures to third parties that are envisaged; given an indication of the period for which the data will be kept, and any other information which may be relevant, ensuring any new or planned projects that involve processing Personal information are preceded with a Data Privacy Impact Assessment.

2. Process the data for the specific and lawful purpose for which it collected that data and not further process the data in a manner incompatible with this purpose.

The CPA will ensure that the reason for which it collected the data originally is the only reason for which it processes those data, unless the individual is informed of any additional processing before it takes place.

3. Ensure that the data is adequate, relevant and not excessive in relation to the purpose for which it is processed.

The CPA will not seek to collect any personal information which is not strictly necessary for the purpose for which it was obtained. Forms for collecting data will always be drafted with this mind. If any irrelevant data are given by individuals, they will be destroyed immediately.

4. Keep personal information accurate and, where necessary, up to date.

The CPA will review and update all data on a regular basis. It is the responsibility of the individuals giving their personal data to ensure that this is accurate, and each individual should notify the CPA if, for example, a change in circumstances mean that the data needs to be updated. It is the responsibility of the CPA to ensure that any notification regarding the change is noted and acted on.

5. Only keep personal data for as long as is necessary.

The CPA undertakes not to retain personal information for longer than is necessary to ensure compliance with the legislation, and any other statutory requirements. This means the CPA will undertake a regular review of the information held and implement a weeding process.

The CPA will dispose of any personal data in a way that protects the rights and privacy of the individual concerned (e.g. secure electronic deletion, shredding and disposal of hard copy files as confidential waste). A log will be kept of the records destroyed.
6. Process personal information in accordance with the rights of the data subject under the legislation.

Individuals have various rights under the legislation including a right to:

- be told the nature of the information the CPA holds and any parties to whom this may be disclosed;
- prevent processing likely to cause damage or distress;
- prevent processing for purposes of direct marketing;
- be informed about the mechanics of any automated decision taking process that will significantly affect them;
- not have significant decisions that will affect them taken solely by automated process;
- sue for compensation if they suffer damage by any contravention of the legislation;
- take action to rectify, block, erase or destroy inaccurate information;
- request that the Office of the Information Commissioner assess whether any provision of the Act has been contravened. The CPA will only process personal information in accordance with individuals’ rights.

7. Put appropriate technical and organisational measures in place against unauthorised or unlawful processing of personal information, and against accidental loss or destruction of information.

All members of staff are responsible for ensuring that any personal information which they hold is kept securely and not disclosed to any unauthorised third parties.

CPA will ensure that all personal information is accessible only to those who have a valid reason for using it. The CPA will have in place appropriate security measures e.g. ensuring that hard copy personal information is kept in lockable filing cabinets/cupboards with controlled access (with the keys then held securely in a key cabinet with controlled access):

- Keeping all personal information in a lockable cabinet with key-controlled access.
- Password protecting personal information held electronically.
- Archiving personal information which are then kept securely (lockable cabinet).
- Placing any PCs or terminals, CCTV camera screens etc. that show personal information so that they are not visible except to authorised staff.
- Ensuring that PC screens are not left unattended without a password protected screen-saver being used.
- Hard drives of redundant PCs will be wiped clean before disposal or if that is not possible, destroyed physically.
- A log will be kept of the records destroyed.

This policy also applies to staff who process personal information ‘off-site’, e.g. when working at home, and in circumstances additional care must be taken regarding the security of the information.

**8) Ensure that no personal information is transferred to a country or a territory outside the European Economic Area (EEA) unless that country or territory ensures adequate level of protection for the rights and freedoms of information subjects in relation to the processing of personal information.**

The CPA will not transfer information to such territories without the explicit consent of the individual. This also applies to publishing membership contact information on the Internet - because transfer of information can include placing information on a website that can be accessed from outside the EEA - so the CPA will always seek the consent of individuals before placing any personal information (including photographs) on its website.

Where the CPA collects personal information in any form via its website, the CPA website has a clear and detailed privacy statement prominently on the website, and wherever else personal information is collected a consent form is available.

In addition, CPA will put in place appropriate measures for the deletion of personal information - manual records will be shredded or disposed of as ‘confidential waste’ and appropriate contract terms will be put in place with any third parties undertaking this work - this is referenced in the CPA Information Retention Policy.
Appendix B Legitimate Interests Assessment Form

The LIA is a light-touch test complete in three parts.

It is not necessary to follow this exact process, but you can use this form to help assess whether legitimate interest can be applied to your processing of personal data.

You should complete and keep a record of this assessment to provide justification for your decision to use legitimate interest as a legal basis before you start processing the data.

<table>
<thead>
<tr>
<th>CPA Activity</th>
<th>Process Name / Description</th>
<th>Data Subject(s)</th>
<th>Nature of personal data processed</th>
<th>Special category, criminal offence or children's data, n/a?</th>
<th>Are the data subjects recorded in the information asset register?</th>
<th>Process owner</th>
<th>Assessment Owner</th>
<th>Assessment Start date</th>
<th>Decision Date</th>
</tr>
</thead>
</table>

1) Purpose: identify the legitimate interest(s). Consider:

| Why do you want to process the data – what are you trying to achieve? |
| Who benefits from the processing? In what way? |
| Are there any wider public benefits to the processing? |
| How important are those benefits? |
| What would the impact be if you couldn't go ahead? |
| Would your use of the data be unethical or unlawful in any way? |
| Have you considered any Tribunal judgements/case law in identifying 'legitimate interests'? |
2) Necessity: apply the necessity test. Consider:

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does this processing actually help to further that interest?</td>
<td></td>
</tr>
<tr>
<td>Is it a reasonable way to go about it?</td>
<td></td>
</tr>
<tr>
<td>Is there another less intrusive way to achieve the same result?</td>
<td></td>
</tr>
<tr>
<td>What is the nature of the CPA’s relationship with the individual?</td>
<td></td>
</tr>
<tr>
<td>Is it pre-existing and have you used their data previously?</td>
<td></td>
</tr>
<tr>
<td>How has the data been obtained? If supplied from a third party what did they tell the individual about reuse?</td>
<td></td>
</tr>
<tr>
<td>Do you have the means and processes to keep the information up to date.</td>
<td></td>
</tr>
<tr>
<td>Is any of the data particularly sensitive or private?</td>
<td></td>
</tr>
<tr>
<td>Would people expect you to use their data in this way?</td>
<td></td>
</tr>
<tr>
<td>Are you happy to explain it to them?</td>
<td></td>
</tr>
<tr>
<td>Are some people likely to object or find it intrusive?</td>
<td></td>
</tr>
<tr>
<td>What is the possible impact on the individual?</td>
<td></td>
</tr>
<tr>
<td>How big an impact might it have on them?</td>
<td></td>
</tr>
<tr>
<td>Are you processing children’s data?</td>
<td></td>
</tr>
<tr>
<td>Are any of the individuals vulnerable in any other way?</td>
<td></td>
</tr>
<tr>
<td>Can you adopt any safeguards and technical measures to minimise the impact?</td>
<td></td>
</tr>
<tr>
<td>Can you offer an opt-out?</td>
<td></td>
</tr>
</tbody>
</table>

**Decision**

<table>
<thead>
<tr>
<th>Outcome Date</th>
<th>Outcome</th>
<th>How was the outcome decided</th>
<th>Further Action</th>
<th>Next Review date</th>
<th>Agreed by</th>
</tr>
</thead>
</table>


Appendix C Data Protection Subject Access Request Form

The Data Protection Act (DPA) 1988 which is replaced on 25th May 2018 by General Information Protection Regulations (GDPR) 2016 gives people the right to see Personal Data held about them by an organisation, by making a Subject Access Request. Please read the guidance notes below before you make your application.

<table>
<thead>
<tr>
<th>Guidance Notes</th>
<th>Do Subject Access Rights Apply?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. Is the information you want about yourself?</strong></td>
<td>Yes</td>
</tr>
<tr>
<td>GDPR allows you to request personally identifiable data about yourself as a “living individual”. Please read our Privacy notice for the types of personal data we collect.</td>
<td></td>
</tr>
<tr>
<td><strong>2. Is the information you want about another person?</strong></td>
<td>Only as described.</td>
</tr>
<tr>
<td>GDPR does not allow you to see the personal data of other people. If you are requesting information about another person, you will need verifiable proof that you are acting on their behalf. Please note this applies to children age 13 years or over also.</td>
<td></td>
</tr>
<tr>
<td><strong>3. Is your request for CCTV footage of you on the Parliamentary Estate?</strong></td>
<td>No</td>
</tr>
<tr>
<td>We are unable to release CCTV footage of you if you have been on the Parliamentary Estate, you will need to contact HM House of Commons, Parliamentary Estate directly.</td>
<td></td>
</tr>
<tr>
<td><strong>4. Requests for personal data by the Police or other statutory bodies.</strong></td>
<td>No</td>
</tr>
<tr>
<td>The Police or other statutory bodies should contact us at <a href="mailto:gdpr@cpahq.org">gdpr@cpahq.org</a></td>
<td></td>
</tr>
</tbody>
</table>
### Section 1 - Contact Details of Requester

<table>
<thead>
<tr>
<th>Name</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td></td>
</tr>
<tr>
<td>Postcode</td>
<td></td>
</tr>
<tr>
<td>Telephone Number</td>
<td></td>
</tr>
<tr>
<td>Email address</td>
<td></td>
</tr>
</tbody>
</table>

**Additional Contact Details**

If you may have been known to us by a different name, address, or email address please provide these details together with the dates to which they may apply below:

---

### Are you the Data Subject? Please tick as appropriate.

The Data Subject is the person whose Personal Data is being requested.

YES □  NO □

### Data Subject Identification

CPA can only release data, if we are satisfied that you are entitled to that information. To help us confirm your identity please provide us with the following:

- **Identification**
  - Please provide an original copy of 1 of the following: Driving License, Birth Certificate, Passport ID, or Medical Card

- **Proof of Address**
  - Please provide a copy of a recent utility bill, or similar, dated within the last 3 months.

### CCTV

If you are requesting CCTV footage we need a written description of you and if you have not already provided photographic ID, a recent photograph of yourself.

**If YES, Please go straight to section 4 of this form.**
Are you acting on behalf of the Data Subject? Please tick as appropriate.
Do you have their express permission, or appropriate legal authority, evidenced in writing?

<table>
<thead>
<tr>
<th>YES</th>
<th>NO</th>
</tr>
</thead>
</table>

IF YES
Please Provide:

- Proof of the Data Subject’s identity, as described above **AND**
- A letter, signed by the Data Subject authorizing you to act on their behalf **OR**
- Evidence of formal legal authority, such as a power of attorney.

Please ensure you also complete Sections 2 and 3 of this form

IF NO
Subject Access Rights do not apply.

---

### Section 2 - Contact Details of Data Subject (if different to those of the Requester in Section 1 above)

<table>
<thead>
<tr>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
</tr>
<tr>
<td>Postcode</td>
</tr>
<tr>
<td>Telephone Number</td>
</tr>
<tr>
<td>Email address</td>
</tr>
</tbody>
</table>
Section 3 – Helping us to find your information

GDPR allows the CPA to request that you provide the information needed to process your application. Please try to specify in the section below, the nature of the information you require.

If you are requesting CCTV, please contact the Parliamentary Estates specifying the location, date and time of the footage as accurately as possible.

Section 4 – Declaration

I certify that the information given on this application form is true and accurate. I understand that making an application for information I am not entitled to may be an offence under GDPR. I understand that it may be necessary for me to provide additional information in order for the CPA to confirm my identity (or that of the Data Subject) and/or locate relevant personal information. I understand that the statutory response period of 30 calendar days, will not commence until the CPA is satisfied of my entitlement.

Signature

Print Name

Date

Section 5 – Submitting your request

Once complete, please send the signed form and copies of any documents to:

Commonwealth Parliamentary Association
CPA Headquarters International Secretariat
First Floor, Room 107
Richmond House
Houses of Parliament
London SW1A 0AA
United Kingdom

Or by email to gdpr@cpahq.org
### Checklist

Please make sure you include the information required to support your request. Our response to you may be delayed if the supporting information is missing.

<table>
<thead>
<tr>
<th>Data Subjects Proof of Identification</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Subjects Proof of Address</td>
<td></td>
</tr>
<tr>
<td>Photo ID for CCTV images of the Data Subject only</td>
<td></td>
</tr>
<tr>
<td>Evidence of authority to act on behalf of the Data Subject</td>
<td></td>
</tr>
</tbody>
</table>

### Section 7 – Disclaimer

Any personal data provided by the CPA in response to your SAR becomes your responsibility once received. We strongly recommend that you keep this information securely and when you no longer need it, ensure it is permanently destroyed.
Appendix D  Data Protection Impact Assessment Template

DPIA author:  
Initiative title:  
Date completed:  

Context

Provide a brief explanation of the initiative - What is the initiative for? When is it likely to happen? How will it provide a benefit to the CPA? How will it provide a benefit to others?

Step One - Identify the need for a DPIA

<table>
<thead>
<tr>
<th>Screening question</th>
<th>Yes/No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does your initiative involve evaluating or scoring individuals (including profiling and predicting)?</td>
<td></td>
</tr>
<tr>
<td>Does your initiative involve automated decision-making that may have a significant effect on an individual?</td>
<td></td>
</tr>
<tr>
<td>Does your initiative involve systematic monitoring?</td>
<td></td>
</tr>
<tr>
<td>Does your initiative involve the processing of sensitive personal data?</td>
<td></td>
</tr>
<tr>
<td>Does your initiative involve processing personal data on a large scale?</td>
<td></td>
</tr>
<tr>
<td>Does your initiative involve datasets that have been matched or combined?</td>
<td></td>
</tr>
<tr>
<td>Does your initiative involve the personal data of vulnerable people?</td>
<td></td>
</tr>
<tr>
<td>Does your initiative involve the use or application of innovative technological or organisational solutions?</td>
<td></td>
</tr>
<tr>
<td>Does your initiative involve the transfer of personal data outside of the European Union?</td>
<td></td>
</tr>
<tr>
<td>Does your initiative prevent individuals from exercising a right or using a service or contract?</td>
<td></td>
</tr>
</tbody>
</table>

Based on the above information, it has been decided that a full DPIA [is/is not] required.
DRAFT

Step Two – Describe the information flows

Step Three – Identify and assess the privacy risks
Please tab to add more rows to the table if needed.

<table>
<thead>
<tr>
<th>Risk ID</th>
<th>Privacy risk</th>
<th>Impact</th>
<th>Likelihood</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Step Four - Identify and approve controls
Please tab to add more rows to the table if needed.

<table>
<thead>
<tr>
<th>Risk ID</th>
<th>Control(s) identified</th>
<th>Expected result</th>
<th>Approved by</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Step Five – Assign responsibility for implementing controls
Please tab to add more rows to the table if needed.

<table>
<thead>
<tr>
<th>Risk ID</th>
<th>Control(s)</th>
<th>Responsible officer</th>
<th>Deadline for implementation</th>
<th>Completion date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Step Six – Reassess and accept the risks
Please tab to add more rows to the table if needed.

<table>
<thead>
<tr>
<th>Risk ID</th>
<th>Privacy risk</th>
<th>Impact after control</th>
<th>Likelihood after control</th>
<th>Risk accepted by</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Consultation

The conduct of this Data Protection Impact Assessment has involved the following consultation:

Contact for raising additional privacy concerns

Name:

Job title:

Email address:  Telephone: