LAW OFFICERS
OF THE CROWN

LAW OFFICERS OF THE CROWN
DATA PROTECTION POLICY

September 2022

Contents

1. **What is Data Protection** 5
2. **Key Definitions** 5
3. **Areas of Responsibility** 8
4. **Data Protection Principles** 9
5. **Acceptable Use and Disclosure** 13
6. **Data Subject Rights** 14
7. **Cross Border Transfers** 15
8. **Processing/sharing information and use of processors** 16
9. **Registration** 17
10. **Breach Notification** 17
11. **Enforcement and Offences** 18
12. **Compliance** 20

APPENDIX 1 21

APPENDIX 2 23

APPENDIX 3 39

About this Policy

This policy must be followed by all members of the Law Officers Chambers (including those on temporary contracts or secondments and covers all aspects of personal data held within Chambers in whatever format that information is held and/or processed.

Everyone has rights with regard to the way in which their personal data is handled. During the course of our activities we will collect, store and process personal data about or obtained from various persons and bodies, including:

(a) the States of Guernsey,
(b) States of Alderney,
(c) Chief Pleas of Sark,
(d) their respective Committees, statutory officers and bodies,
(e) providers of services (including tax, housing, health, social care, education and children services),
(f) Law Enforcement agencies within and outside the Bailiwick of Guernsey,
(g) the Crown,
(h) departments of the Government of the United Kingdom,
(i) the courts and judiciary,
(j) the general public dealing or involved with those entities and services,
(k) suppliers, and
(l) other third parties.

The Law Officers of the Crown including HM Receiver General ("the Law Officers") as data controllers have obligations under the Data Protection (Bailiwick of Guernsey) Law, 2017 and associated legislation in relation to data protection. We recognise that the correct and lawful treatment of this data will maintain confidence in the Law Officers of the Crown as an organisation and will assist and demonstrate best practice and compliance. The same considerations apply to the handling of the personal data of our staff.

This policy may be amended at any time. Any breach of this policy (read in conjunction with any other States of Guernsey IT directions/policies and the staff employee handbook) may result in disciplinary action.

Personal data processed (see definitions section) by or on behalf of the Law Officers on paper, on a computer or other media is subject to legal safeguards specified in the Data Protection (Bailiwick of Guernsey) Law, 2017 and associated legislation (such as the Data Protection (Law Enforcement and Related Matters) (Bailiwick of Guernsey) Ordinance, 2018. One of the very few exceptions is a situation where the data is not processed by automated means and does not form and is not intended to form part of a filing system.

This policy and any other documents referred to in it set out the basis on which every member of the Law Officers Chambers will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources. This Policy will focus primarily on the requirements of the Data Protection (Bailiwick of Guernsey) Law, 2017.

Please note that the bulk of the 2017 Law does not apply to processing by a competent agency for law enforcement purposes. The applicable law for such agencies is the Data Protection (Law Enforcement and Related Matters) (Bailiwick of Guernsey) Ordinance, 2018 ("**the 2018 Ordinance**"). The main underlying definitions and principles, however, are broadly applicable in the processing of all personal data in Chambers.

The Working Practice Requirements (set out in Appendix 1) must be followed by all staff.

This policy has been approved by the Law Officers and members of their Senior Management Team. It sets out our rules on data protection and the legal conditions that must be satisfied when we obtain, handle, transfer, store or otherwise process personal data.

If you consider that the policy has not been adhered to in respect of personal data about yourself or others you should raise the matter with your line manager or the Data Protection Guardian.

The policy will be reviewed as required but at a minimum frequency of every two years or if any changes to the law occur that require review of the policy.

1. What is Data Protection

1.1 Generally, the purpose of the Law is to protect the rights of living individuals in relation to their personal data and ensure that their personal data is not processed unlawfully.

1.2 Most personal data processed by or on behalf of the Law Officers in the discharge of our functions falls within the definition of privileged items and is exempt from data subject rights and controller's duties set out in in Part III of the Law (see below Data Subject Rights). However, even where such data is subject to legal professional privilege, members of Chambers share a responsibility to take reasonable steps to ensure personal data, in particular special category data, is kept secure and that there is no unlawful disclosure and/or processing of such data. This includes compliance with the Data Protection Principles set out in section 4 of this policy.

2. Key Definitions

2.1 Data protection relates to personal data, the type of information about an individual which each of us would consider personal to us. 'Personal data' is defined by the Data Protection (Bailiwick of Guernsey) Law, 2017 ("**the Law**") as follows:-

"**Personal data**" means any information relating to an identified or identifiable individual.

An individual is identifiable from any information where the individual can be directly or indirectly identified from the information, including –

(a) by reference to a name or an identifier,
(b) by reference to one or more factors specific to the person's physical, physiological, genetic, mental, economic, cultural or social identity,
(c) where, despite pseudonymisation, that information is capable of being attributed to that individual by the use of additional information, or
(d) by any other means reasonably likely to be used, taking into account objective factors such as technological factors and the cost and amount of time required for identification in the light of the available technology at the time of processing.

Personal data that is controlled under the Law comprises data held in all formats including, but not limited to, the following:

- Documents, presentations and spreadsheets stored digitally
- Paper based files
- Emails
- Backup and archive systems
- CCTV recordings
- Audio and video recordings

For more guidance as to what is personal data please press 'Control' and click here.

2.2 "**special category data**" means –

(a) personal data revealing an individual's –
  (i) racial or ethnic origin,
  (ii) political opinion,
  (iii) religious or philosophical belief, or
  (iv) trade union membership,
(b) genetic data,
(c) biometric data,
(d) health data,
(e) personal data concerning an individual's sex life or sexual orientation, or
(f) criminal data.

In simple terms, special category data is personal data that needs more protection because it is sensitive. Special category data can only be processed under strict conditions.

2.3 Other terms common to data protection are listed below together with a definition.

"**controller**" –

(a) means a person that, alone or jointly with others, determines the purposes and means of the processing of any personal data, and
(b) for the avoidance of doubt, includes a processor or any other person, where the processor or other person determines the purposes and means of processing personal data.

The Law Officers (HM Procureur and HM Comptroller) are the data controllers in respect of St James Chambers for the purposes of the Law.

The "**Data Protection Authority**" is responsible for the Law and its administration throughout the Bailiwick. The Authority is independent of the States of Guernsey. Usually, the Commissioner (known colloquially as the Data Protection Commissioner) exercises the functions of the Authority on a day-to-day basis. Occasionally you may see a reference to "ODPA" which is a colloquial reference to the Office of the Data Protection Authority.

"**data subject**", in relation to personal data, means the identified or identifiable individual to whom the personal data relates,

"**filing system**" means any structured set of personal data which is accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis. The Law applies only where personal data is processed by automated means or the personal data forms or is intended to form part of a filing system.

"**processor**" –

(a) means an individual or other person that processes personal data on behalf of a controller, and
(b) includes a secondary processor within the meaning of section 36(1) of the Law,

"**processing**" –

(a) means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, for example –
(i) collection, recording, organisation, structuring or storage,
(ii) adaptation or alteration,
(iii) retrieval, consultation or use,
(iv) disclosure by transmission, dissemination or otherwise making available,
(v) alignment or combination, or
(vi) restriction, erasure or destruction,

(b) includes any further or continued processing of personal data, falling within paragraph (a), and
(c) for the avoidance of doubt, includes profiling,

"**third party**", in relation to any processing of personal data, means a person other than–

(a) the data subject, controller or processor, or
(b) a person who, under the direct authority of the controller or processor, is authorised to process the personal data.

"**privileged items**", means items subject to legal professional privilege within the meaning given by section 24 of the Police Powers and Criminal Evidence (Bailiwick of Guernsey) Law 2003 (i.e. communications between a professional legal adviser and the advisor's client made in connection with the giving of legal advice or with or in contemplation of legal proceedings) and any communications between a professional legal advisor and the advisor's client in connection with the giving of legal advice to the client with respect to the client's duties, liabilities or rights under the Law.

"**lawful processing**" – in Appendix 2 to this policy we have included the full text of Schedule 2 to the Law which sets out the conditions for the processing of personal data to be lawful and Schedule 2 to the Data Protection (General Provisions) (Bailiwick of Guernsey) Regulations, 2018 which sets out circumstances of authorised processing by certain controllers. Please note that the conditions for lawful processing of special category data by a competent agency for law enforcement purpose are set out in Schedule 2 to the 2018 Ordinance.

3. Areas of Responsibility

3.1 Every member of the Law Officers Chambers has a responsibility for data protection compliance.

3.2 **The Data Protection Officer** (DPO) for the Law Officers is currently the person assigned to this role by the Head of the Data Protection Team of the States of Guernsey (currently Sam Nichols). The DPO's functions are set out in sections 50 and 51 of the Law. These include:

- Informing and advising the Law Officers, the Director of Legal Services and Chambers' staff of their duties under the Law and any other laws relating to data protection;
- Monitoring the Law Officers' compliance with the Law, any other laws relating to data protection, this Policy (including awareness raising and training);
- Reporting directly to the Senior Management Team of Chambers;
- Advising on data protection impact assessments if required and requested;
- Acting as contact point with the Authority; and
- Cooperating with the Authority in the exercise of its functions.

3.3 **The Chambers Data Protection Guardian** (currently Nick Whalley):

- Reports to the Director of Legal Services;
- Manages the registration of the Law Officers with the Authority (including making any returns required);
- Ensures that the Chambers' Information Asset Register (IAR) and retention policy is completed and then regularly reviewed, preferably every 12 months thereafter;
- Ensures that any matters/work arising from review of the IAR are completed as far as practicable within a reasonable timeframe;
- Ensures that the Chambers Data Protection policy is completed and then regularly reviewed, preferably every 2 years thereafter;
- Ensuring and monitoring compliance by Chambers staff with the Working Practice Requirements set out in Appendix 1 of this policy;
- Working and liaising with the Chambers SAR lead and Chambers DPO in managing the response to any request for information (SAR) received by Chambers;
- Maintaining contact with Chambers DPO in relation to training, SOG practices and general advice in relation to data protection;
- Liaising with relevant Chambers staff in relation to relevant legal issues;
- Organising and attending the quarterly Chambers data protection knowledge group meetings; and

- If at any time a risk of conflict of interest arises in relation to a particular issue, must inform the Director of Legal Services who will as necessary substitute an alternative member of staff.

3.4 **The Chambers SAR lead** (currently Penny Grainge):

- Reports to the Director of Legal Services;
- Is the first point of contact within Chambers in relation to any right of access request (commonly known as Subject Access Requests) received by a member of Chambers;
- Is the single point of contact with Chambers DPO and coordinates the response to the SAR;
- Liaises with the Chambers DPO and the Law Officers in relation to the SAR response;
- In case of risk of conflict of interest, can be substituted in the case of a particular SAR by the Director of Legal Services; and
- Determines the overall approach and provision of a response to the SAR, including any matters raised by the ODPA.

3.5 **The Director of Legal Services**:

- Is responsible on behalf of the Law Officers for compliance with the Law and the 2018 Ordinance and this policy;
- Oversees the management of data protection matters;
- Ensures reporting lines exist to allow both the Data Protection Guardian and the Data Protection Officer to raise matters at senior management level.

3.6 All staff in carrying out their work duties have a responsibility to ensure compliance with the principles of the Law, this Policy and any applicable States of Guernsey policies relating to data / record retention and all legally qualified staff have a duty to ensure that in giving advice to clients, data protection issues are identified and further advice or information sought as appropriate.

3.7 All staff have a duty to ensure compliance with the working practice requirements set out in Appendix 1.

4. Data Protection Principles

4.1 There are seven principles governing data protection and the processing of personal data.

4.2 The seven principles are listed below with an explanation of each one and the effect each has on data processing.

4.3 Please note that the data protection principles that apply to agencies for law enforcement purposes are set out in sections 4 to 11 of the 2018 Ordinance. These principles are slightly different to those set out below.

4.4 **Principal 1 – Lawfulness, Fairness and Transparency**

"Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject"

4.4.1 This principle is key to the processing of personal data. All data must be processed fairly and transparently, and lawfully (in accordance with one or more of the conditions in Schedule 2 to the Law – see Appendix 2 to this policy).

4.4.2 In the case of special category data, the Law imposes stricter conditions (to reflect the more sensitive nature of that data) and requires at least one condition in Part II or III of Appendix 1 must be satisfied. In any other case, at least one condition in Part I or II of that appendix must be satisfied. Exceptionally, there special circumstances in which processing is specially authorised by regulations: see Schedule 2 to the Data Protection (General Provisions) (Bailiwick of Guernsey) Regulations, 2018. Schedule 2 to the Law and Schedule 2 to those regulations are set out in Appendix 2 to this policy.

4.4.3 Fair processing is to ensure, where possible, that all data subjects are aware of the personal data being processed, for what purpose and what that processing may involve. Please press 'Control' and click here for access to the Fair Processing Notice of the Law Officers and here for the Fair Processing Notice of HM Receiver General.

4.4.4 The use of more specific fair processing notices is encouraged, particularly where personal data is collected directly from the data subject by or on behalf of the Law Officers (or a client of the Law Officers).

4.4.5 Whether or not personal data is processed fairly must also be determined by having regard to the method by which it is obtained, including whether any person from whom it is obtained is deceived or misled as to the purpose or purposes for which it is to be processed. One example of fairly obtained personal data is data that is required or authorised to be supplied by or under an enactment.

4.4.6 It is imperative that personal data is processed lawfully. It is not acceptable for a Chambers member of staff to obtain or process personal data for reasons other than for lawful purposes related to the functions of the Law Officers.

4.5 **Principle 2 – Purpose Limitation**

"Personal data: (i) must not be collected except for a specific, explicit and legitimate purpose, and (ii) once collected, must not be further processed in a manner incompatible with the purpose for which it was collected."

4.5.1 Personal data should be collected for one or more specified purposes (satisfying the conditions referred to in paragraphs 3.3.1 and 3.3.2 above). Data should not be used for any other purpose that is incompatible with the purpose for which it was originally collected. Whether or not personal data is further processed in a manner that is incompatible with the purpose for which it was collected must be determined having regard to the "proportionality factors" set out in paragraph 4 of Schedule 9 to the Law. These factors include, inter alia, the nature of the data including whether it is special category data, the characteristics of the data subject including whether or not the subject is a child, the reasonable expectation of the data subject and the possible consequences of the processing for the data subject.

4.5.2 The further processing is deemed to be compatible with the original purpose of collection if (i) the explicit consent of the data subject is obtained for the further processing; (ii) the further processing is for a historical or scientific purpose; or (iii) the further processing is specifically authorised or required by an enactment. By way of example, in accordance with section 27 of the Children (Guernsey and Alderney) Law, 2008, ("**the 2008** Law") employees of the States of Guernsey and all other persons have a duty whilst working with a child they reasonably believe to be a child in need or at risk to take such action in relation to that child as may be required of them under the 2008 Law. Where to discharge that duty an employee or other person is obliged to disclose to another person, retain or otherwise deal with information relating to an individual, such processing would be required by the 2008 Law and as such be deemed compatible with the original purpose of collection.

4.5.3 It is therefore imperative that members of staff are clear as to the basis upon which they have access to, hold or are using data in the course of their duties. Qualified staff will be expected to ensure that those deputies, civil servants or others who they are advising are also aware of this principle, particularly in those areas where special category data may also be involved.

4.6 **Principle 3 – Minimisation**

"Personal data processed must be adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed".

4.6.1 Information held by the Law Officers Chambers must be suitable for the purpose for which it is required.

4.6.2 It is not appropriate to hold data 'just in case'. However, it is acceptable to hold data for which there is a set purpose and with lawful occasion to use but that it is uncertain if and when that occasion may arise. For example, we may hold data of the next of kin of staff members for use in the event of an emergency and/or we may hold data given to us by clients which they consider relevant for the purpose of seeking advice from us.

4.6.3 Personal data may be in the form of facts and opinions. It is however important to distinguish between the two when recording it. It should be remembered that it is not always relevant to record an opinion. It should always be clear when an opinion has been expressed / recorded. The recording of an opinion that is then mistaken as fact by others may result in distress or upset being caused to the data subject.

4.6.4 Excessive personal data and data that is not required should not be collected or processed. Unrelated data should not be requested and held just because it is seen as an ideal opportunity to obtain as much information as possible.

4.7 **Principle 4 – Accuracy**

"Personal data processed must be accurate and where applicable, kept up to date, and reasonable steps must be taken to ensure that personal data that is inaccurate (having regard to the purpose for which it is processed) is erased or corrected without delay…"

4.7.1 There is an obligation to ensure that data is accurate and kept up to date, so far as applicable.

4.7.2 Records should be updated with new information whenever it is appropriate to accurately reflect the current position.

4.8 **Principle 5 – Storage Limitation**

"Personal data must not be kept in a form that permits identification of the data subject any longer than is necessary for the purpose for which it is processed (but may be stored longer to the extent necessary for a historical or scientific purpose)."

4.8.1 Data should not be retained for longer than is required and must be reviewed on a regular basis. Different data can be retained for different lengths of time. For example, information on a serious criminal matter may be retained indefinitely whereas other records may be subject to frequent review and destruction.

4.8.2 The Law Officers' Chambers has a Data Retention Policy which should be followed.

4.9 **Principle 6 – Integrity and Confidentiality**

> "Personal data must be processed in a manner that ensures its security appropriately, including protecting it against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

4.9.1 This principle is concerned with ensuring the confidentiality, availability and integrity of data. This is to make sure it is secure, available for use by those that need it and can be relied upon as accurate. Under the Law, controllers must take reasonable steps to ensure a level of security appropriate to the personal data.

4.9.2 Information should be held securely when not being used and disposed of with due consideration of confidentiality. Encryption and Passwords for all computer systems and mobile devices should be robust, information should not be emailed or transported without adequate security and information should be made available only to those that legitimately and lawfully require it.

4.9.3 The accidental loss or theft of personal data has been identified as key risk for Chambers and all staff must be particularly careful when handling and transporting documents or other media containing personal data, and if personal data is removed outside the office for example on memory sticks, laptops or hard copy documents. The loss of such data would not only cause significant reputational damage to Chambers but could also incur a significant fine and adverse publicity.

4.10 **Principle 7 – Accountability**

> "The controller is responsible for, and must be able to demonstrate, compliance with the data protection principles […]"

4.10.1 This principle requires the Law Officers to be able to demonstrate that we are complying with all the other data protection principles. Where practicable, steps taken to ensure compliance with the data protection principles should be recorded so that we can demonstrate compliance if queried.

5. Acceptable Use and Disclosure

5.1 Personal data is processed by Chambers staff solely to give advice to clients and other persons and bodies who seek advice and to enable the Law Officers to discharge their functions. Please refer to the Fair Processing Notices (paragraph 4.4.3 above).

5.2 When processing personal data users should have the seven principles in mind. Any person who is not certain or confident around the application of the Law (or the 2018 Ordinance) in any particular circumstance should seek advice and assistance.

6. Data Subject Rights

6.1 Part III of the Law sets out the rights of data subjects in relation to their personal data. (See Part III of the 2018 Ordinance in the case of data held by a competent agency for law enforcement purposes – the provisions are slightly different.) As set out above, much (but not all) of the personal data held by or on behalf of the Law Officers will be exempt from the rights under Part III as such data will be subject to legal professional privilege or one of the other exemptions prescribed in Schedule 8 to the Law. However it will always be necessary to review items carefully to establish whether or not they are privileged and whether or not other exemptions apply. Also it should be remembered that in relation to legal advice privilege, it is usually the case that correspondence sent by members of Chambers to, or received by members of Chambers from, third parties who are not our clients will not attract privilege.

6.2 Under the Law data subjects have, inter alia, the following rights with regard to their personal data:

6.3 **The right of access to their personal data –** this is not a right to receive copies of any document held containing personal data about the data subject. It is a right to be given confirmation as to whether or not personal data relating to that data subject is being processed and to be given a copy of that personal data – not necessarily any document within which such data is held.

6.4 **The right to rectification –** to ask for incorrect or inaccurate information to be rectified.

6.5 **The right to erase or to restrict -** to ask for personal data to be deleted or removed or for processing to be blocked or restricted for a period of time.

6.6 **The right to information about personal data collected –** to be informed that personal data is held and/or being processed, the reason why and the lawful basis.

Please note that in the event that personal data is collected (directly from the individual or indirectly from elsewhere within the States of Guernsey or other authorities/agencies), that does not come within the definition of privileged items (or one of the other exemptions to Part III of the Law (Data Subject Rights) which are set out in Schedule 8 to the Law), we will have a responsibility to give prescribed information to the data subject. This prescribed information is set out in Schedule 3 to the Law. An example where this responsibility may arise could be correspondence between Chambers and a third party (non-client) in connection with a data subject, other than in connection with or contemplation of proceedings.

6.7 Please note that the general exceptions and exemptions from Part III of the Law and Part II of the 2018 Ordinance are set out in Schedule 8 to the Law and Schedule 3 to the Ordinance respectively.

7. Cross Border Transfers

7.1 Personal data should not be transferred to any country or territory unless:

(a) the country or territory is listed in Appendix 3 of the Policy; or, if not,
(b) you are satisfied that at least one of the conditions in 7.2 below is met.

7.2
(a) where there are sufficient safeguards (e.g. legally binding agreement, binding and approved corporate rules, standard data protection clauses, approved code or approved mechanism) and a mechanism for data subjects to enforce data subject rights and obtain legal remedies against the transferee;
(b) where the transfer is authorised by the Data Protection Authority;
(c) where required to do so by a court or tribunal order;
(d) where required to do so by a decision of a public authority based on an international agreement binding on the Bailiwick;
(e) where required to do so by law, in accordance with an order or decision of a foreign court or tribunal, or foreign public authority, based on an international agreement binding on the Bailiwick;
(f) where the data subject has given explicit and informed consent to the transfer;
(g) where the transfer is necessary for the conclusion or performance of a contract in the interest of the data subject or to which the data subject is a party, or to take steps requested by the data subject prior to entering into such a contract;
(h) the transfer is necessary for or in connection with legal proceedings, to obtain legal advice or to establish, exercise or defend legal rights;
(i) where the transfer is necessary to protect the life, health or safety of an individual and the controller cannot reasonably be expected to obtain the explicit consent of the data subject (or the data subject is physically or legally incapable of giving consent);
(j) where the personal data is in a public register; or in a register to which certain members of the public have conditional access and the transfer is at the request of such a member who has such access to the personal data;
(k) where the transfer is non-repetitive, concerns a limited number of data subjects, is necessary for compelling legitimate interests that outweigh the data subjects' interests and the applicable safeguards are assessed to be appropriate;
(l) where the transfer is to a British jurisdiction designated by Ordinance as an authorised jurisdiction (the UK is currently designated as an 'authorised jurisdiction, pending an 'adequacy' declaration for the UK by the European Commission); or
(m) where the transfer is authorised by Regulations made by the Committee for Home Affairs (currently only transfers by the Guernsey Financial Services Commission or the Stock Exchange are so authorised, where required or

authorised by or under an enactment, and even then subject to specified conditions – see Schedule 3 to the Data Protection (General Provisions) (Bailiwick of Guernsey) Regulations, 2018)

7.3 For the avoidance of doubt, following the decision of the Court of Justice of the European Union in Schrems II, the US Privacy Shield is no longer considered to provide "sufficient safeguards" (within the meaning of 7.2 (a) above) for the transfer of personal data to the United States of America. Transfer to the USA will be considered unlawful unless other safeguards (e.g. standard contractual clauses that are "sufficient") apply or another condition in 7.2 is satisfied.

7.4 Where personal data is transferred based on one of the conditions in paragraph 7.2, a written record should be kept of the transfer and the condition on which it is based.

7.5 The need for an information agreement or arrangement should be considered as set out in paragraph 8.2 below.

7.6 Advice should be sought from Chambers DPO in relation to a proposed transfer of any data to a country or territory not listed in Appendix 3, if you are confident that one of the conditions set out in in paragraph 7.2 is satisfied.

8. Processing/sharing information and use of processors

8.1 The Law Officers of the Crown (including HM Receiver General) are an independent data controller as are States' Committees and other bodies. The legal bases on which personal data may be processed is set out in paragraphs 6 and 7 of the Fair Processing Notices which can be found on the Law Officers website (see paragraph 4.4.3 for the links). Personal data may only be disclosed to the recipients listed in paragraph 8 of each Fair Processing Notice where necessary for a purpose mentioned in paragraphs 6 and 7 of the notice.

8.2 The Law Officers, where necessary, should enter into information sharing agreements with other controllers. If there is a regular exchange of personal data, an information sharing agreement should be drafted or used to ensure that data is handled to a standard that meets the requirements of the Law Officers. There are UK based templates available that could be adopted for Bailiwick use which can be obtained from Chambers DPO. If there is an ad-hoc exchange or disclosure of personal data, no contract is necessary (although consideration should still be given to this) but some written form of assurance should be sought that the data will be handled in a confidential fashion and in compliance with the Law.

8.3 Where a processor is used or commissioned by the Law Officers, sufficient guarantees or a legally binding agreement must be concluded with the processor. Advice on templates can be obtained from Chambers DPO. For example, there is pending a controller-processor agreement between the Law Officers and Phoenix Business Solutions, the company that maintains our Document Management System.

9. Registration

9.1 In order to process personal data, it is necessary for an organisation to be registered with the Data Protection Authority. Failure to register when so required is a criminal offence (section 39(3)).

9.2 As indicated in paragraph 8.1 above the Law Officers are registered with the Data Protection Authority and our registration (including making any returns required) is managed by the Data Protection Guardian should anyone wish to view it.

10. Breach Notification

10.1 A "**personal data breach**" is a breach of security leading to:

(a) accidental or unlawful destruction, loss, or alteration of, or
(b) unauthorised disclosure of, or access to,
personal data.

10.2 All personal data breaches of which staff become aware of must be reported to the Data Guardian. The Data Guardian must keep written records of each data breach reported to him or her including:

a) the facts relating to the breach,
b) the effects of the breach (if any),
c) the remedial action taken, and
d) any steps taken by the Law Officers as controllers or the Data Guardian on behalf of the Law Officers, to comply with the Law including where necessary giving notice of the breach to the Data Protection Authority.

10.3 A personal data breach can include:

- sending an email containing personal data to an incorrect recipient,
- an unauthorised third party accessing electronic or hardcopy documents containing personal data,
- a computing device or USB key or other removable media containing personal data being lost or stolen,
- a hardcopy document containing personal data being lost or stolen or given to an incorrect/unauthorised recipient.

10.4 When staff report a personal data breach to the Data Guardian they must, in addition to outlining points a) to c) above, give an assessment of whether the breach is likely or unlikely to result in any risk to the significant interests of the data subject

concerned. By way of example, an email containing personal data sent to the incorrect recipient but one who is an employee of the States of Guernsey or a Chambers staff member may not result in any risk to the significant interests of the data subject concerned, if remedial action is taken swiftly by way of that person deleting the email from their inbox and emptying it from their 'Deleted items' folder.

10.5 The Data Guardian will inform the Law Officers and the Director of Legal Services of all breaches reported to the Data Guardian.

10.6 Where a personal data breach is likely to result in a risk to the significant interests of the data subject, written notice of the same must be given to the Data Protection Authority as soon as practicable and in any event no later than 72 hours after becoming aware of the breach, unless this is not practicable, in which case an explanation for the reason for the delay will be needed.

10.7 The Data Guardian in consultation with the staff member, and on taking legal advice and/or advice from the DPO if considered necessary, must consider whether the breach must be reported in writing to the Data Protection Authority.

10.8 If the assessment is that the breach is likely to result in a risk to the significant interests of the data subject, or, in the event, for whatever reason, an assessment is not undertaken, the Data Guardian must immediately inform the Law Officers, the Director of Legal Services and the DPO in writing of the breach. The DPO will then report the breach in writing to the Authority.

10.9 In addition the DPO must notify the data subject concerned in writing of a personal data breach that has been reported. This notification must be made as soon as possible.

10.10 Both the UK Information Commissioner and the Data Protection Authority have issued guidance in relation to personal data breaches and reporting. Please press 'Control' and click here and then here for further information.

11. Enforcement and Offences

11.1 On receipt of a complaint that a controller or processor has acted or is likely to act in breach of the Law, the Data Protection Authority has a duty to investigate and make a determination as to whether there has been or is likely to be a breach. The Authority may also launch an investigation on its own initiative, without receipt of a complaint. If after an investigation the Authority determines there has been a breach, the Authority may issue a reprimand and/or impose an administrative fine or impose a whole range of other sanctions on the controller or processor concerned.

11.2 Where there are been a breach determination, the Authority may also serve an enforcement notice. It is also possible for civil proceedings for breach of operative provisions of the Law, including in respect of data subject rights, to be brought by either the Authority or the aggrieved individual/data subject.

11.3 There are also a number of criminal offences that may arise as a result of breaches of operative provisions of the Law.

11.4 **Enforcement Notices**

11.4.1 An enforcement notice may specify certain actions that must be carried out within a certain time and/or request an organisation to refrain from processing any stated personal data in any stated manner for a period of time.

11.4.2 An enforcement notice can be cancelled or varied by the Data Protection Authority.

11.4.3 The serving of an enforcement notice can be appealed.

11.4.4 Failure to comply with an enforcement notice is a criminal offence (section 73(6) of the Law).

11.5 **Criminal Offences**

11.5.1 In most cases, potential liability for any criminal offence arising from breaches of the Law will lie with the Law Officers as controllers. By way of example, failure to comply with an enforcement notice, failure to notify the Data Protection Authority of changes to Chambers registration particulars and the processing of personal data without registration (unless otherwise exempt).

11.5.2 There are in addition, however, areas in which potential criminal liability could arise *personally* for a member of staff within Chambers. Knowingly or recklessly obtaining or disclosing, procuring to another or retaining personal data without the consent of the data controller is a criminal offence (section 87). This does not apply, however, to a person who shows:

a) that the obtaining, disclosing, procuring or retaining was required or authorised by law,
b) that the person acted in the reasonable belief that it was so required or authorised by law,
c) that the person acted in the belief that they would have had the consent of the controller if the controller had known of the obtaining, disclosing, procuring or retaining, and the surrounding circumstances,
d) that the obtaining, disclosing, procuring or retaining was for a law enforcement purpose,

e) that the exception relating to journalism, or artistic, literary of academic purpose applies (see section 87(2)(d) of the Law), or
f) that in the particular circumstances, the obtaining, disclosing, procuring or retaining was justified in the public interest.

11.5.3 Intentionally obstructing a Data Protection Authority official in the course of exercising their function without reasonable excuse or interfering with or removing anything secured by an Authority official in the course of exercising their function is also a criminal offence (section 88).

12. Compliance

12.1 Compliance with this policy will be monitored by the Data Protection Guardian.

APPENDIX 1
WORKING PRACTICE REQUIREMENTS

Specific data protection requirements of the Law Officers Chambers (these apply not only to personal data, but the keeping and processing of any data generally):

Electronic / Hard Copy Data

All work-related electronic data must be saved to the appropriate workspace within Chambers Document Management System ("DMS"). To ensure it is possible to effectively locate personal data, it would be helpful that all DMS workspaces and all documents relating to an individual not in a personally named workspace, are named with a data subject's full name. For ease of retrieval, therefore, initials should not be used for the naming of documents (save when referring to members of staff) unless those documents are to be saved to a workspace in the name of an individual data subject. Initials should not be used for the naming of workspaces which are opened in the name of an individual data subject.

Work containing personal data should not be saved to a shared drive (i.e. H drive) or local drives (i.e. C drive) or any removable media except where there is good reason (for, example, in relation to removeable media, where documents cannot be emailed due to size). Work containing personal data should not be saved to desktop other than for a very short period of time. If work is not immediately saved to the appropriate workspace on DMS, it must be so saved as soon as practical thereafter.

Where practicable all hard copy data must be converted to electronic format (scanned) and saved to DMS.

Electronic Mail (Email)

Particular care must be taken when sending an e-mail containing data whereby the loss, misuse, modification or unauthorised access to sensitive information can adversely affect legal privilege, the privacy or welfare of an individual, trade secrets of a business or the security, internal and foreign affairs of the Bailiwick of Guernsey. This will depend on the level of sensitivity and nature of the information. This includes e-mail containing 'special category data' as defined by the Data Protection (Bailiwick of Guernsey) Law, 2017 (see section 2.2 above).

Staff must not email work containing personal data to their personal email addresses or to the personal email addresses of other employees of the States of Guernsey, Deputies or other organisations. Work containing personal data should not be emailed to a personal email address of an individual without confirmation that the email address is in fact that of the individual concerned.

IT security

Staff must not share passwords. Whenever staff leave their desk, they must lock their screens (hold down windows key then L key).

Removable media

Removable media comes in the form of USB keys, CD-ROM/DVD and external hard drives and should only be used for work purposes if absolutely necessary, e.g. the criminal team viewing CCTV footage. The Admin team keep a small stock of USB keys and these are controlled by way of a register and must be signed out and in by a member of the Admin team. Every effort should be made to ensure the security of removable media whilst being transported or otherwise outside the office.

Transporting Hard Copy Documents

If hard copy documents must be taken outside Chambers, staff should ensure they are held securely in a file and every effort must be made to ensure the security and confidentiality of the documents whilst they are outside the office.

Storage of hardcopy documents containing personal data

All hard copy documents containing personal data must be stored in locked cabinets.

Clear Desk Policy

Chambers operates a clear desk policy and staff should endeavour to ensure their desks are clear of any client related work at the end of each day and ensure that no hardcopy documents containing personal data are left on their desks at the end of each day.

Chambers security

Keys and tags must be kept secure at all times and not lent or given to non-Chambers staff.

Working from home

Chambers staff must ensure that these working practices are followed whilst working from home.

These working practice requirements address the specific situations that may arise in the Law Officers Chambers but must be read alongside the more detailed States Directives on Email, IT Security, Removable Media, Mobile Computing etc. Please press 'Control' and click here for reference.

APPENDIX 2
CONDITIONS FOR LAWFUL PROCESSING

It should be noted that each condition applies separately on its own (i.e. the scope and application of any one condition does not depend on the scope or application of another condition).

Sort out the E.g. just because processing falls outside (or is excluded from) one condition does not automatically mean that it falls outside another condition.

Schedule 2 to the Data Protection (Bailiwick of Guernsey) Law, 2017

CONDITIONS FOR PROCESSING TO BE LAWFUL

The following are conditions for processing to be lawful –

Part I (non-special category data only)

1. The data subject has requested or given consent to the processing of the personal data for the purpose for which it is processed.

2. The processing is necessary –

   (a) for the conclusion or performance of a contract –
      (i) to which the data subject is a party, or
      (ii) made between the controller and a third party in the interest of the data subject, or
   (b) to take steps at the request of the data subject prior to entering into such a contract.

3. The processing is necessary to protect the vital interests of the data subject or any other individual.

4. The processing is necessary for the purposes of the legitimate interests of the controller or a third party, except where the processing is in the context of the exercise or performance by a public authority of a function or task described in paragraph 5.

5. The processing is necessary for the exercise or performance by a public authority of –

   (a) a function that is of a public nature, or
   (b) a task carried out in the public interest.

6. The processing is necessary for the controller to exercise any right or power, or

perform or comply with any duty, conferred or imposed on the controller by law, otherwise than by an enactment or an order or a judgment of a court or tribunal having the force of law in the Bailiwick.

Part II (special category or non-special category data)

7. The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

8. The processing is necessary for the controller to exercise any right or power, or perform or comply with any duty, conferred or imposed on the controller by an enactment.

9. The processing is necessary in order to comply with an order or a judgment of a court or tribunal having the force of law in the Bailiwick.

10. (a) The processing is necessary for a health or social care purpose and is undertaken by –

(i) a health professional, or
(ii) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if the person were a health professional.

(b) In subparagraph (a) –

"**health or social care purpose**" includes the purpose of –

(i) preventative or occupational medicine,
(ii) the assessment of the working capacity of an employee or worker,
(iii) medical diagnosis,
(iv) the provision of medical, health or social care or treatment, or
(v) the management of medical, health or social care systems and services.

11. (a) The processing –

(i) is necessary for reasons of public health, for example –
(A) for protection against serious threats to public health, or
(B) to ensure high standards of quality and safety for health care, medicinal products or medical devices, and
(ii) is carried out with appropriate safeguards for the significant interests of data subjects.

(b) In subparagraph (a)(i)(B) –

"**medical device**" means–

(i) any medical device, within the meaning of Article 1(2)(a) of Council Directive 93/42/EEC of 14 June 1993 concerning medical devices, or

(ii) any accessory, within the meaning of Article 1(2)(b) of that Council Directive, and

"**medicinal product**" has the meaning given by section 133 of the Medicines (Human and Veterinary) (Bailiwick of Guernsey) Law, 2 0 0 8 .

12. The processing is necessary –

(a) for the purpose of, or in connection with –

(i) any legal proceedings (including prospective legal proceedings), or

(ii) the discharge of any functions of a court or tribunal acting in its judicial capacity,

(b) for the purpose of obtaining legal advice, or

(c) otherwise for the purposes of establishing, exercising or defending legal rights.

13. The processing is necessary for –

(a) the administration of justice, or

(b) the exercise of any function of the Crown, a Law Officer of the Crown, the States or a public committee.

13A. The processing is necessary for a law enforcement purpose.

14. The processing –

(a) is in the context of the legitimate activities of any person which –

(i) is not an individual,

(ii) is not established or conducted for profit, and

(iii) exists for political, philosophical, religious or trade-union purposes,

(b) is carried out with appropriate safeguards for the significant interests of data subjects,

(c) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and

(d) does not involve disclosure of the personal data to a third party without the consent of the data subject.

15. The processing is necessary for a historical or scientific purpose.

16. This condition is satisfied if the condition in subparagraph (a) is satisfied, subject to subparagraphs (b) and (c) –

(a) The personal data processed is of a category specified in the left-hand column of the table below, and the processing is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between the groups of people specified in the right-hand column of that table in relation to each category of personal data, with a view to enabling such equality to be promoted or maintained:

Category of personal data	**Groups of people (in relation to a category of personal data)**
Personal data revealing racial or ethnic origin	People of different racial or ethnic origin
Personal data revealing religious or philosophical beliefs	People holding different religious or philosophical beliefs
Health data	People with different states of health
Personal data concerning an individual's sexual orientation	People of different sexual orientation

(b) Processing does not satisfy the condition in subparagraph (a) if it is carried out –

(i) in order to make a decision, or facilitate or allow a decision to be made, with respect to a particular data subject, or

(ii) in such a way that substantial damage is, or is likely to be, caused to any data subject.

(c) Processing does not satisfy the condition in subparagraph (a) if –

(i) a data subject has given notice in writing to the controller requiring the controller not to process the personal data, and has not given notice in writing withdrawing that requirement,

(ii) the notice gave the controller a reasonable period in which to stop processing such data, and

(iii) that period has ended.

17. The processing is –

(a) authorised by regulations made by the Committee for this purpose and carried out in accordance with those regulations, or

(b) authorised or required by any other enactment and carried out in accordance with the enactment.

Part III (special category data)

18. The data subject has given explicit consent to the processing of the personal data for the purpose for which it is processed.

19. The processing is necessary to protect the vital interests of the data subject or any other individual, and –

(a) the data subject is physically or legally incapable of giving consent, or
(b) the controller cannot reasonably be expected to obtain the explicit consent of the data subject.

Schedule 2 to the Data Protection (General Provisions) (Bailiwick of Guernsey) Regulations, 2018

AUTHORISED PROCESSING OF PERSONAL DATA

	Column 1	**Column 2**	**Column 3**	**Column 4**
Row.	**Personal data**	**Controller**	**Purposes**	**Conditions**
1.	Personal data relating to the name and address of the registered keeper of an abandoned motor vehicle	The Environment Committee	Enabling or facilitating the owner or occupier of the land on which the vehicle is abandoned to take action to enable the removal or disposal of the vehicle	The following conditions must be satisfied – (a) the processing is by way of disclosure by the Environment Committee, (b) the registered keeper is physically or legally incapable of giving consent to the disclosure, or the Environment Committee cannot reasonably be expected to obtain the consent of the registered keeper, and (c) the disclosure is made on terms and conditions determined by the Environment Committee after consulting the Authority.
2.	Personal data concerning any employee,	STSC or a STSC-related body	Enabling or facilitating STSC to carry out a	-

	Column 1	Column 2	Column 3	Column 4
Row.	**Personal data**	**Controller**	**Purposes**	**Conditions**
	debtor or creditor of a STSC-related body, excluding any special category data		relevant function of the STSC-related body	
2A.	Any personal data	Any committee of the States of Guernsey, or any public committee (within the meaning of s. 111(1) of the Data Protection (Bailiwick of Guernsey) Law, 2017) of the States of Guernsey in receipt of public funds, (collectively a "**scrutinised committee**") to which a request for information is made by or on behalf of the Scrutiny Management Committee ("**Scrutiny Committee**") of the States of Guernsey in carrying out its function* of leading and coordinating the scrutiny of that committee ("**its scrutiny function**"). *For the avoidance of doubt, this provision applies even if the request is made for the purpose of a review or an inquiry	To assist or facilitate the Scrutiny Committee to carry out its scrutiny function, in response to the request for information.	Personal data must not be disclosed to the Scrutiny Committee unless – (a) that committee undertakes not to process any of that personal data other than as necessary for the purpose of carrying out its scrutiny function or any other purpose contemplated by a fair processing notice given to the scrutinised committee, and (b) further, in the case of personal data relating to any data subject other than a member of a scrutinised committee, that committee undertakes not to publish that personal data without the consent of the data subject concerned.

	Column 1	Column 2	Column 3	Column 4
Row.	**Personal data**	**Controller**	**Purposes**	**Conditions**
		commenced by the Scrutiny Committee (in the exercise of its scrutiny function) before the commencement of the Data Protection (General Provisions) (Bailiwick of Guernsey) (Amendment) Regulations, 2020.		
3.	Special category data	Any person acting for or on behalf of – (a) Ofsted, or (b) a person, service or institution in the Bailiwick being inspected by or on behalf of Ofsted	Enabling or facilitating an inspection relating to any person, service or institution in the Bailiwick carried out by or on behalf of Ofsted further to an approved arrangement	The approved arrangement must contain safeguards in relation to any personal data processed for the purpose of the inspection.
4.	Special category data	Any person providing confidential counselling, advice, support or other similar service provided confidentially	Providing or delivering services of the kind specified in column 2	The processing – (a) needs to be carried out without the data subject's consent – (i) because the data subject is physically or legally incapable of giving consent, (ii) because the controller cannot reasonably be expected to obtain the consent of the data subject, or (iii) in order not to prejudice the purpose in column 3, and (b) is in the public interest.

	Column 1	Column 2	Column 3	Column 4
Row.	**Personal data**	**Controller**	**Purposes**	**Conditions**
5.	Health data or criminal data	Any person carrying on insurance business, or acting for or on behalf of such a person	Enabling or facilitating the person to carry on insurance business	The processing – (a) is necessary for a purpose relating to an objective that is in the public interest, and (b) where condition A applies, satisfies condition B. Condition A applies where– (a) the processing is not carried out for the purposes of measures or decisions with respect to the data subject, and (b) the data subject does not have and is not expected to acquire – (i) rights against, or obligations in relation to, an insured person under an insurance contract entered into by or on behalf of the controller, or (ii) any other rights or obligations in connection with such a contract. Condition B is satisfied if the controller - (a) cannot reasonably be expected to obtain the consent of the data subject, and

	Column 1	Column 2	Column 3	Column 4
Row.	**Personal data**	**Controller**	**Purposes**	**Conditions**
				(b) the controller is not aware of the data subject withholding consent.
6.	Health data relating to a data subject who is the parent, grandparent, great grandparent or sibling of a member of a pension scheme.	Any person making determinations in connection with eligibility for, and benefits payable under, a pension scheme	Enabling or facilitating the person to make determinations of the kind specified in column 2	The processing – (a) needs to be carried out without the data subject's consent – (i) because the data subject is physically or legally incapable of giving consent, or (ii) because the controller cannot reasonably be expected to obtain the consent of the data subject, and (b) does not support measures or decisions affecting the significant interests of the data subject.
7.	Criminal data	Any person	A purpose in connection with any of the following – (a) the recruitment of an individual as an employee, (b) the continued employment of an individual, (c) any contract for the provision of services to the controller by another person, or (d) the provision (for payment or not) of goods, facilities or	The processing – (a) is required or authorised by law, or (b) in the circumstances, is justified as being in the public interest.

	Column 1	Column 2	Column 3	Column 4
Row.	**Personal data**	**Controller**	**Purposes**	**Conditions**
			services to the public or any section of the public	
8.	Special category data	Any person	Exercising any right or power, or performing or complying with any duty, conferred or imposed by law on the controller in connection with employment	-
9.	Special category data	An elected representative	Carrying out any function as an elected representative	The processing – (a) is carried out pursuant to a request made by the data subject to the elected representative to take action on behalf of the data subject or any other individual, and (b) is necessary for the purposes of, or in connection with, the action reasonably taken by the elected representative pursuant to that request.
10.	Special category data	An elected representative	Carrying out any function as an elected representative	The processing – (a) is carried out pursuant to a request made by an individual other than the data subject to the elected representative to take action on behalf of the data subject or any other individual, (b) is necessary for the purposes of, or in

	Column 1	Column 2	Column 3	Column 4
Row.	**Personal data**	**Controller**	**Purposes**	**Conditions**
				connection with, the action reasonably taken by the elected representative pursuant to that request, and (c) needs to be carried out without the data subject's consent – (i) because the data subject is physically or legally incapable of giving consent, (ii) because the controller cannot reasonably be expected to obtain the consent of the data subject, (iii) in order to protect or safeguard the significant interests of another individual, in any case where the data subject has unreasonably withheld consent, or (iv) in order not to prejudice the action taken by the elected representative pursuant to that request.
11.	Special category data	Any person	Responding to a communication to the controller made by an elected representative pursuant to a request made by the data subject	The processing – (a) consists of a disclosure of special category data to the elected representative, and (b) the special category data is relevant to the communication specified in column 3

	Column 1	Column 2	Column 3	Column 4
Row.	**Personal data**	**Controller**	**Purposes**	**Conditions**
12.	Special category data	Any person	Responding to a communication to the controller made by an elected representative pursuant to a request made by an individual other than the data subject	The processing – (a) consists of a disclosure of special category data to the elected representative, (b) the special category data is relevant to the communication specified in column 3, and (c) needs to be carried out without the data subject's consent – (i) because the data subject is physically or legally incapable of giving consent, (ii) because the controller cannot reasonably be expected to obtain the consent of the data subject, (iii) in order to protect or safeguard the significant interests of another individual, in any case where the data subject has unreasonably withheld consent, or (iv) in order not to prejudice any action taken by the elected representative pursuant to that request.
13.	Special category data	Any person	The prevention, detection or investigation of any unlawful act or omission	The processing – (a) needs to be carried out without the data subject's consent in order not to prejudice

	Column 1	Column 2	Column 3	Column 4
Row.	**Personal data**	**Controller**	**Purposes**	**Conditions**
				the purpose in column 3, and (b) is in the public interest.
13A.	Any personal data	Any controller	Publication of a judgment or other decision of a court or tribunal	The processing – (a) consists of the publication of such a judgment or decision, or (b) enables or facilitates the publication of such a judgment or decision.
14.	Any personal data	Any person discharging a protective function	Properly discharging the protective function	The processing – (a) needs to be carried out without the data subject's consent in order not to prejudice the purpose in column 3, and (b) is in the public interest.
15.	Any personal data	A police officer	Exercising or performing any function conferred or imposed on the police officer by any rule of law or customary law	-
16.	Any personal data	Public authority	Identifying or assessing the risk to the Bailiwick of money laundering, terrorist financing, breaches of international sanctions or other forms of financial crime.	The processing needs to be carried out in order to maintain the reputation and standing of the Bailiwick.

In this Schedule –

"**abandoned motor vehicle**" means a motor vehicle which appears to have been abandoned on privately owned land without the permission of the owner or occupier of that land,

"**approved arrangement**" means a written arrangement entered into between Ofsted and any public committee,

"**criminal data**" means personal data relating to –

(a) the commission or alleged commission of a criminal offence by an individual, or

(b) proceedings for a criminal offence committed or alleged to have been committed by an individual, the disposal of such proceedings or the sentence of a court in such proceedings,

"**the Environment Committee**" means the States of Guernsey Committee for Environment & Infrastructure,

"**in the context of employment**" has the meaning given by section 105(3) of the Law,

"**insurance business**" has the meaning given by Schedule 5 to the Insurance Business (Bailiwick of Guernsey) Law, 2002,

"**insurance contract**" means a contract of general insurance or long-term insurance,

"**insured person**" includes an individual who is seeking to become an insured person,

"**member of a pension scheme**" includes an individual who is seeking to become a member a pension scheme,

"**occupier**" means any person occupying land under a lease for a term of at least 12 months,

"**Ofsted**" means the Office for Standards in Education, Children's Services and Skills of the United Kingdom,

"**pension scheme**" has the meaning given by section 2(1)(e) of the Regulation of Fiduciaries, Administration Businesses and Company Directors, etc. (Bailiwick of Guernsey) Law, 2000,

"**protective function**" has the meaning given by paragraph 15 of Schedule 8 to the Law,

"**registered keeper**", in relation to a motor vehicle, means the person in respect of whom the motor vehicle is for the time being registered under the Motor Taxation and Licensing (Guernsey) Law, 1987,

"**relevant function**" means a function that the STSC has agreed with any STSC-related body, or any person acting on behalf of such a body, that the STSC will carry out on behalf of the STSC-related body,

"**STSC**" –

(a) means the division or part of the States of Guernsey Policy & Resources Committee known as the Shared Transactional Service Centre, which is responsible for administering and implementing policies approved by the States of Deliberation for the delivery of shared services, and

(b) includes any successor of that division or part to which those functions are delegated or assigned, and

"**STSC-related body**" means –

(a) a public committee of the States of Guernsey or States of Alderney, or

(b) any other person to which the STSC delivers services.

APPENDIX 3
COUNTRIES AND TERRITORIES TO WHICH PERSONAL DATA CAN BE TRANSFERRED

Countries to which Personal Data can be transferred:

European Union Member States:

Austria
Belgium
Bulgaria
Croatia
Republic of Cyprus
Czech Republic
Denmark
Estonia
Finland
France
Germany
Greece
Hungary
Ireland
Italy
Latvia
Lithuania
Luxembourg
Malta
Netherlands
Poland
Portugal
Romania
Slovakia
Slovenia
Spain
Sweden

Countries declared to be an Authorised Jurisdiction

The United Kingdom

Countries/Jurisdictions Declared to be Adequate:

Andorra
Argentina
Canada (commercial organisations)
Faroe Islands
Guernsey
Isle of Man
Israel
Jersey
New Zealand
Switzerland
Uruguay