1 Personal Data Policy

The SG seeks to develop and maintain positive relationships with data subjects. We explicitly state our purposes for personal data; define our consent management approach and identify any intention to supply personal data to third parties.

While we can process some personal data under assumed or implicit consent, we prefer consent to be explicit to inform our data subjects and to maintain a clear link between our headline purposes and our data management actions. Explicit consent is usually essential for sensitive personal data.

A suitably worded consent clause will identify:

- The Scottish Government as data controller
- A lead business area nominee as the 'data owner'
- Our purpose(s) for processing the personal data
- Any legislation or statute relevant to the data collection
- Any third parties we intend to supply with personal data.
- Any third party data purposes where these vary from the SG ones
- Our consent approach for the personal data purposes

We are accountable for our data management actions and decisions.

Where possible we inform data subjects of our purpose(s) during data capture, this is the most effective point to confirm data content and quality as obtaining retrospective permissions or corrections can be a costly and difficult exercise. We always seek consent where a choice exists and identify any legal statute driving our requests for personal data.

We obtain personal data only when necessary for specified purposes, while data remains personal and identifiable we use it only for those purposes. Legitimate use depends on purpose, data content and consent management. Holding personal data for one purpose grants no right of use for any unconnected purpose.

We can compel the supply of personal data in very few contexts, when we can use it only for a compelling purpose. We obtain more and better quality personal data by consent management than any attempt to compel. Compulsion is costly, it reduces data quality and quantity and restricts re-use and so we avoid it where possible.

If a new purpose arises after the data collection we can sometimes process existing data without a retrospective permissions exercise if this 'further purpose' is not 'incompatible with the purposes for which they (the data) were obtained' and a fair balance can be struck between the legitimate interests of the data controller and the data subjects. To do this we must record the decision, noting the data and purposes and our perception of the balance of interests and risks. This can only ever be a temporary measure; future consent management must cover all known purposes.

1.1 How does the Data Protection Act apply to SG?

The Data Protection Act applies to the Scottish Government, The Scotland Act extends the terms 'a Minister of the Crown' to the Scottish Ministers and 'government department' to the Scottish Government. The Scottish Government corporate data controller is the Scottish Government, day-to-day data and processing responsibility falls to nominated senior managers, named to data subjects as the contact for data protection purposes.

1.2 What is Personal Data?

"Personal Data" relates to a living individual who can be identified -

(a) from those data, or

(b) from those data and other information in the possession of, or likely to come into the possession of, the data controller,

This includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

1.3 When can we process Personal Data?

We can only process personal data when a Data Protection Act Schedule 2 condition is satisfied;

- The individual has given consent to the processing
- The processing is necessary for the performance of a contract with the individual
- The processing is required under a legal obligation
- The processing is necessary to protect the vital interests of the individual
- The processing is necessary for the administration of justice, for the exercise of any functions conferred by enactment or for the exercise of any functions of a Minister of the Crown or government department
- The processing is necessary for the pursuit of the legitimate interests of the data controller or certain third parties (unless prejudicial to the interests of the individual).

1.4 What is Sensitive Personal Data?

Stricter conditions apply to the processing of 'sensitive personal data', which is individually identifiable information relating to;

- Racial or ethnic origin
- Mental or Physical Health
- Sex Life
- Political Opinions

- Religious or other beliefs
- Trade union Member ship
- Crimes, allegations, offences, court proceedings

1.5 When can we process Sensitive Personal Data?

To process sensitive personal data a controller must meet at least one Schedule 2 condition and at least one from Schedule 3 of the Act:

- The individual has given explicit consent to the processing
- The processing is necessary for a legal obligation in connection with employment
- The processing is necessary to protect the vital interests of the data subject or another person where consent: cannot be given, cannot reasonably be obtained, or is unreasonably withheld, by or on behalf of the data subject.
- The processing is for the legitimate activities of a not for profit organisation, a political, philosophical, religious or trade union body. (Does not apply to the Scottish Government.)
- The information contained in the personal data was made public as a result of steps deliberately taken by the data subject.
- The processing is necessary for the purpose of legal proceedings or prospective proceedings, to obtain legal advice and establish, exercise or defend legal rights.
- The processing is necessary for the administration of justice, for the exercise of any functions conferred by enactment or for the exercise of any functions of a Minister of the Crown or government department
- The processing is necessary for medical purposes and undertaken by a health professional, or a person who owes a duty of confidentiality equivalent to that of a health professional. "Medical purposes" include preventative medicine, medical diagnosis and research, the provision of care and treatment and management of healthcare services.
- The processing is of racial or ethnic origin data, and is necessary to identify or review equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enable, promote or maintain equality and done with appropriate safeguards for the rights and freedoms of data subjects.
- The personal data are processed in circumstances specified in an order made by the Secretary of State for the purposes of this paragraph

How do we obtain consent for our purposes?

We must inform data subjects of our purposes and seek consent to process personal data for these. Consent for sensitive data use must be explicit. We cannot assume consent from a supply or presence of data or absence of a refusal. We must ensure data subjects do have a choice of consent in the supply and use of their data and so we must allow for refusals, partial supply and nil returns of data.

1.6 Can I match, link and supply personal data?

- Personal data linking always requires data subject consent as this can be prejudicial to the interests of the individual.
- We have no right to link individual personal data to other individual personal data without data subject consent.
- Consent must be explicit if the scope of the purpose, personal identifiers or data items has the potential to include sensitive information.
- We have no right to process personal data for any purpose incompatible with the purposes for which we originally obtain the data, non-consented personal data linkage will always be an incompatible purpose.
- We do not supply or disclose personal identifiers or identifying data (including name and date of birth) unless necessary for a purpose that has data subject consent.

1.7 What must we do to protect personal data?

The data controller must take appropriate technical and organisational measures to safeguard personal data.

- Personal data must be disposed of appropriately when it is no longer required for a purpose.
- Where appropriate personal data must be kept accurate and up to date
- The data controller must support data-subject access requests.
- All data processors must take precautions against unauthorised or unlawful processing, supply, disclosure or disposal of personal data.
- We impose similar conditions on any third party we supply with personal data.
- We must secure personal data and only disclose, disseminate, and dispose of it appropriately.
- We must train staff in the appropriate personal data management procedures before they can handle any personal data in any format.

1.8 Can a third party process SG personal data?

Before a third party can process data on our behalf,

- a written contract must exist to state the processor agrees to act only on the instructions of the controller and
- abide by appropriate provisions to meet the security principles in full.

Defining appropriate purposes and security standards is essential to support any third party processing contract.

The Scottish Government remains the data controller where it controls the data and processing purpose.

We can supply personal data for third party own account purposes if the third party and their purposes are identified to the data subjects and consent is obtained.

1.9 What is personal data disclosure?

Disclosure is the term for a personal data use, including

- capture
- storage
- reading
- processing
- supply

All disclosures require data subject consent or an over-riding reason for not obtaining this. We abide by data subject consent for the purposes we identify at data capture or at the point of disclosure

1.10 When is data 'necessary' or 'excessive'?

All personal data must be required for a purpose. We obtain and supply personal data only when it is necessary for a purpose.

Where it is necessary to process a data item for a purpose that data is required, each personal data item must pass this test.

We respect data subject rights of consent to supply 'optional' data, this is personal data that we process when present but it is not essential to our purpose; an example is a request for age or sex, when this is not essential to supply a service but will profile the uptake to inform on or improve service targets.

We only obtain the personal data items we require for our processing purposes; any more will be excessive, redundant or unnecessary.

- For age analysis, an age or age band will be necessary, but a date of

birth is not.

- To contact a data subject a contact address is necessary, we cannot insist on home address.
- To contact data subjects during the working day a daytime contact is necessary, an evening one will be excessive.
- We may request non-essential items only if we identify they are optional and data subjects can opt out of supply.
- We must intend to process each data item; unless each data item has a purpose it is redundant.
- We only supply personal identifiers or data to third parties where necessary and for a consented purpose.
- We remove all unnecessary personal data and identifiers before we supply personal data to any third party.

Excessive data can increase data management costs, raise business and personal risks, compromise data subject rights and reduce the utility of our data.

1.11 Is data 'necessary' for a function of government?

The term 'necessary for a function of government' does not give government a right to personal data; the SG informs data subjects of our purposes and their rights. We must identify a specific 'function of government' purpose and cite any legal position we rely upon to obtain or use personal data. If a statute does not require a personal data item, we cannot insist on its supply and must seek it by consent. A legitimate interest may not always translate into a legal right to obtain personal data.

1.12 Do we need training to handle Personal Data?

Yes, all staff must be trained before they can handle personal information in any form in the course of their job. We recommend this basic entry level training is part of the staff induction process.

Business areas must supply specific desk instructions and train staff in these before staff can handle any personal data in any format: on computer, electronic media, in structured files, e-mail or correspondence

1.13 Who are the Scottish Government data subjects?

If we hold identifiable data on a person they are a data subject, we describe these in the Data Protection Act Register. Scottish Government data subjects include:

- Customers
- Staff /Employees
- Contractors/Advisers
- Offenders
- Farmers
- Suppliers
- Teachers
- Pupils/Students
- Ministers

As the scope of personal data held in the Scottish Government is very wide so the potential to link individual data from different sources is also very wide.

1.14 What is a data purpose in the Scottish Government?

A data purpose is why we process personal data. We obtain personal data for one or more identified purpose(s). We identify purpose(s) to our data subjects and register these with ICO.

Scottish Government purposes include:

- Administration
- Staff management
- Contract management
- Training
- Employment
- Statistics and Research
- Planning
- Education
- Justice/Crime
- Pay/Pensions/Tax
- Environment
- Health/Welfare

If an appropriate purpose is not on this list, we must update our entry. Purposes 'not incompatible' with a specified purpose may also be appropriate.

1.15 What is a compatible data purpose?

Statistical or management information purposes can be compatible when they inform on an administration purpose; if the analysis will not identify individuals or support decisions directly affecting them. Future data collections must identify any extension to our purposes and apply appropriate consent management.

Personal data linking is never a compatible purpose; we always require consent for individual data linkage. Two separate individual data purpose consents do not add up to a right to link the two sets of individual data; you will need consent for a linking purpose. Consent must be free and fair: we cannot offer incentives or use pressure to influence the data subject in their consent decisions.