SPCB Privacy Notice

This privacy notice explains how we handle personal data in connection with the Security Questionnaire.

About Us
The Data Controller is the Scottish Parliament Corporate Body (SPCB).

The Data Protection Officer for the Scottish Parliament is the Head of Information Governance:

Contact information and further advice

If you have any further questions about the way in which we process personal data, or about how to exercise your rights, please contact the Head of Information and Governance at:

The Scottish Parliament, Edinburgh, EH99 1SP

Telephone: 0131 348 6913 (Text Relay calls and calls in British Sign Language through contactscotland-bsl.org welcome)

Email: dataprotection@parliament.scot

Collection of your personal data
The personal data collected for the purposes of this notice are those specified on this form. We may also collect data about you from the Police National Computer database (criminal records – both spent and unspent as defined by the Rehabilitation of Offenders Act 1974) and the Security Service.

Use of your personal data
The lawful basis for collecting and using the personal data described above is that it is necessary for a task carried out in the public interest.

The personal data we collect on this form is collected for the purposes of security (physical, cyber and information), including conducting baseline protective security standard checks, national security vetting, and managing access to the parliamentary estate and IT network.

Furthermore, depending on the circumstances, the processing may also be necessary for the performance of a contract, or steps required to be taken prior to the entering into a contract. This is the case because a successful processing of the security questionnaire is a pre-requisite to taking up employment with the SPCB.

A further lawful basis is required when processing special categories of data may include Criminal Record details and Financial Checks.

Criminal offence data is special category data. The processing of criminal offence data for the purpose of the security questionnaire is necessary for a task carried out
with substantial public interest. The substantial public interest is the safety and security of the Scottish Parliament building and its occupants.

- for substantial public interest purposes; or
- for employment, social security and social protection purposes.

We may also use your personal data and special category data to protect your vital interests or the vital interests of others you are associated with, if it were to become necessary, for example, whilst visiting the parliamentary campus. Details about the lawful basis for processing personal data can be found on the Information Commissioner’s website [here](#).

**Storage and retention of your personal data**
The Scottish Parliament will retain your personal data for as long as is necessary for the purpose it was collected. In most cases, a retention period will apply which can be found in the Scottish Parliament’s [Authorised Records Disposal Policy](#) on our website.

For the purposes of this notice, your personal data will be retained for such time as you:

- are in possession of a valid security pass granting access to the parliamentary campus
- have access to the parliamentary IT network;

Your personal data will be disposed of, securely, one year after date of leaving the Parliament.

**Disclosure and security of your personal data**
We may disclose your personal data to third parties when permitted to do so including:

- where we have a contract with a processor acting on our behalf;
- if we have a lawful basis for doing so;
- if we are under a duty to disclose or share your personal data in order to comply with any legal obligation. This includes providing your personal data to other organisations, such as the police, for the purposes of prevention and detection of crime with your instruction or consent.

Your personal data may be shared with, and checked against, data held by the police and law enforcement agencies, the Security Service and credit reference agencies.
We will never share or sell your personal data to other organisations for direct marketing purposes.
All personal data you provide will be stored securely, both physically and electronically, in accordance with our policies. We have an information security process in place to oversee the effective and secure processing of your personal data.
Where we use third party processors, we ensure appropriate contracts and duty of confidentiality are in place and technical and organisational measures to ensure the security of data have been assessed as appropriate.
Personal data is held within the UK.
Your rights
We will ensure you can exercise your rights in relation to the personal data you provide to us. These may include:

- You can request access to the personal data we hold about you at any time by contacting the Data Protection Officer whose contact details are found at the top of this notice (subject to limited exceptions which include information collected for the purposes of national security vetting).
- You can ask us to update your personal data if it changes. In certain circumstances, you can request we erase the personal data we hold, or ask us to stop or restrict processing if you have an objection (subject to limited exceptions).
- If you have any privacy-related questions or unresolved problems relating to the use of your personal data, you may contact us to complain by contacting the Data Protection Officer whose contact details are found at the top of this notice.
- You also have the right to complain to the Information Commissioner’s Office, the supervisory authority, about our collection and use of your personal data.

They can be contact at
Information Commissioner’s Office,
Wycliffe House,
Water Lane,
Wilmslow,
Cheshire,
SK9 5AF, www.ico.org.uk.
Further details about your rights and the complaints process can be found on the Information Commissioner’s website here.