JUDICIAL APPOINTMENTS BOARD FOR SCOTLAND

DATA PROTECTION POLICY

This document represents policy and procedures for data protection as approved by the Judicial Appointments Board for Scotland on Date.

The policy was last reviewed by the Board on Date.

(signed) ……
Governance Manager

Statement: I have read and agree to abide by the procedures set out in this document.

(signed)…… (Board/Secretariat Member)

NAME (please print) ……..

JUDICIAL APPOINTMENTS BOARD FOR SCOTLAND

DATA PROTECTION POLICY

1. Introduction

The Judicial Appointments Board for Scotland (JABS) is committed to protecting the rights and freedoms of data subjects and safely and securely processing their data in accordance with all of our legal obligations.

We hold personal data about our employees, applicants for Judicial Office, suppliers and other individuals for a variety of business purposes.

This policy sets out how we seek to protect personal data and ensure that our Board Members and staff understand the rules governing their use of the personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the Data Protection Officer (DPO), John Wallace, be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

The Data Protection Act 2018 (the 2018 Act) contains a number of exemptions from the requirements of the General Data Protection Regulation (GDPR) where personal data is processed for the purposes of assessing a person's suitability for judicial office. The exemptions concern the requirements of the GDPR to provide information to those who provide us with their personal data, to access personal data, rectification, erasure and restriction of processing.

Good Data Protection practice is not just a matter of legal compliance and ticking the boxes. Data Protection is about taking care of people and respecting their privacy. Protecting the confidentiality and integrity of personal data is a critical responsibility that we take seriously at all times. The correct and lawful treatment of personal data will maintain confidence in JABS, will provide for successful business operations, and will maintain the reputation of JABS. If JABS fails to comply with data protection law, this could not only harm individuals, but may expose JABS to substantial sanctions and/or reputational damage.

2. Definitions

Business purposes	The purposes for which personal data may be used by us: Personnel, administrative, financial, regulatory, payroll and business development purposes. Business purposes include the following: - Compliance with our legal, regulatory and corporate governance obligations and good practice - Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests - Ensuring business policies are adhered to (such as policies covering email and internet use) - Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting,

	credit scoring and checking
	- Investigating complaints
	- Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments
	  - Monitoring staff conduct, disciplinary matters
	  - Marketing our appointment rounds
	  - Improving services
	  - Assessing suitability for judicial office
	  - Discharging our statutory functions

Personal data	'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal data includes special category personal data (see below), personal data relating to criminal offences and criminal convictions and pseudonymised personal data but excludes anonymous data or data that has had the identity of the individual permanently removed. Personal data can be a fact (e.g. a name, email address, location or date of birth) and/or an opinion about a person. **Personal data we gather may include***: individuals' phone number, email address, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.*
Special categories of personal data	Special categories of personal data include information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-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 —any use of special categories of personal data should be strictly controlled in accordance with this policy.
Data controller	'Data controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines where, why and how to process personal data. It is responsible for establishing practices and policies in

	line with data protection law. JABS is the data controller of all personal data relating to JABS personnel and personal data used in our business for our own business purposes.
Data processor	'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Processing	'Processing' 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, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Supervisory authority	This is the national body responsible for data protection. The supervisory authority in the UK is the **Information Commissioners Office (ICO)**.
Anonymisation	This is a valuable tool that allows data to be shared, whilst preserving privacy. The process of anonymising data requires that identifiers are changed in some way such as being removed, substituted, distorted, generalised or aggregated.
Pseudonymisation	This is a procedure where personally identifiable information fields within a data record are replaced by one or more artificial identifiers, or pseudonyms.

3. Our Legal Basis for using people's data

Everything we do with records about individuals – obtaining the information, storing it, using it, sharing it, and even deleting it – must have an acceptable legal basis. There are five legal bases on which we rely for processing personal data:

I. Consent from the individual (or someone authorised to consent on their behalf) to the processing of his or her personal data for one or more specific purposes.
II. Where processing is necessary for the performance of a contract between JABS and the individual.
III. Where processing is necessary for compliance with a legal obligation to which JABS is subject.
IV. Where processing is necessary to protect the vital interests of the individual or another natural person.
V. Where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in JABS.

Under Section 9 of the Judiciary and Courts (Scotland) Act 2008, the Judicial Appointments Board for Scotland (the Board) has statutory functions to recommend individuals for appointment to judicial offices within the Board's remit and to provide advice in connection with such appointments. This policy has been framed by reference to JABS's statutory functions.

4. Data Protection Principles

Subject to exemptions provided by the 2018 Act, JABS shall comply with the principles of data protection (the Principles) enumerated in the EU General Data Protection Regulation. We are responsible for and must be able to demonstrate compliance with these principles. The Principles are:

Lawful, fair and transparent
Processed lawfully, fairly and in a transparent manner.

Limited for its purpose
Collected only for specified, explicit and legitimate purposes, and processed only in line with those purposes;

Data minimisation
Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

Accurate
Accurate and, where necessary, kept up to date.

Retention
Not kept in a form which permits identification of individuals for longer than necessary, in relation to the purposes for which it is processed.

Security, integrity and confidentiality
Kept secure, and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

5. Accountability and Transparency

We must ensure accountability and transparency in all our use of personal data. We must show how we comply with each Principle. We are responsible for keeping a written record of how all the data processing activities we are responsible for comply with each of the Principles. This must be kept up to date and must be approved by the DPO.

To comply with data protection laws and the accountability and transparency Principle of GDPR, we must demonstrate compliance. The Board and staff are responsible for understanding their particular responsibilities to ensure we meet the following data protection obligations:

- Fully implement all appropriate technical and organisational data protection measures

- Maintain up to date, accurate and relevant documentation on all processing activities
- Conducting Data Protection Impact Assessments
- Implement measures to ensure privacy by design and default, including:
    - Data minimisation
    - Pseudonymisation
    - Transparency
    - Allowing individuals to check processing regularly for accuracy, relevancy and that the information remains up to date, subject to exemptions provided by the 2018 Act
    - Creating and improving security and enhanced privacy procedures on an ongoing basis

6. Special Categories of Personal Data

Previously known as sensitive personal data, this means data about an individual which is more sensitive, so requires more protection. This type of data could create more significant risks to a person's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination. The special categories include information about an individual's:

- race
- ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data (where used for ID purposes)
- health
- sex life and sexual orientation

The Board does seek some of this data from applicants: typically their physical or mental health, sexual orientation, religion and racial or ethnic origin by asking applicants to fill in a voluntary diversity monitoring form.

Under section 14 of the Judiciary and Courts (Scotland) Act 2008, the Board has a statutory duty to have regard to the need to encourage diversity in the range of individuals available for selection to be recommended for appointment for judicial office.

The GDPR sets out the conditions for the fair processing of special categories of personal data. One of these conditions requires the data subject giving his or her explicit consent for the processing of the data. It is the Board's policy to seek such consent on the application form.

The condition for processing special categories of personal data must comply with the law. If we do not have a lawful basis for processing special categories of data that processing activity must cease and the data must be destroyed.

7. Responsibilities

The Board will take good care of the information that we hold, whether in digital form or on paper, and will ensure that guidance and training will be provided so that data and information are treated in line with data protection law.

In particular, the Board's responsibilities will be:

- Analysing and documenting the type of personal data we hold
- Checking procedures to ensure they cover all the rights of the individual
- Identify the lawful basis for processing data including special category personal data
- Ensuring consent procedures are lawful
- Implementing, reviewing and enforcing procedures to detect, report and investigate personal data breaches
- Storing data in safe and secure ways
- Assessing the risk that could be posed to individual rights and freedoms should data be compromised
- Ensuring all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Researching third-party services, such as cloud services the company is considering using to store or process data
- Approving data protection statements attached to emails and other marketing copy
- Addressing data protection queries from clients, target audiences or media outlets
- Coordinating with the Data Protection Officer to ensure all marketing initiatives adhere to data protection laws and the company's Data Protection Policy

Staff and Board Members will:

- Fully understand their data protection obligations
- Check that any data processing activities they are dealing with comply with our policy and are justified
- Not use data in any unlawful way
- Not store data incorrectly, be careless with it or otherwise cause us to breach data protection laws and our policies through their actions
- Comply with this policy at all times

- Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations to the DPO without delay
- Attend training on this policy

Responsibilities of the Data Protection Officer (DPO):

- Keeping the Board updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection training and advice for all staff members and those included in this policy
- Answering questions on data protection from staff, board members and other stakeholders
- Responding to individuals such as clients and employees who wish to know which data is being held on them by us, subject to exemptions provided by the 2018 Act
- Checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing
- Reporting data protection breaches to ICO

Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Subject to exemptions provided by the 2018 Act, individuals may ask that we correct inaccurate personal data relating to them. If the Board or staff believe that information is inaccurate they should record the fact that the accuracy of the information is disputed and inform the DPO.

8. Rights of individuals

Subject to exemptions provided by the 2018 Act, individuals have rights to their data which we must respect and comply with.

We will facilitate the exercise of rights by individuals in the following ways:

Right to be informed

- Providing privacy notices which are concise, transparent, intelligible and easily accessible, free of charge, that are written in clear and plain language, particularly if aimed at children.
- Keeping a record of how we use personal data to demonstrate compliance with the need for accountability and transparency.

Right of access

- Enabling individuals to access their personal data and supplementary information
- Allowing individuals to be aware of and verify the lawfulness of the processing activities

Right to rectification

- We must rectify or amend the personal data of the individual if requested because it is inaccurate or incomplete.
- This must be done without delay, and no later than one month. This can be extended to two months with permission from the DPO.

Right to erasure

- We must delete or remove an individual's data if requested and there is no compelling reason for its continued processing.
- Inaccurate data must be corrected or deleted without delay.

Right to restrict processing

- We must comply with any request to restrict, block, or otherwise suppress the processing of personal data.
- We are permitted to store personal data if it has been restricted, but not process it further. We must retain enough data to ensure the right to restriction is respected in the future.

Right to data portability

- We must provide individuals with their data so that they can reuse it for their own purposes or across different services.
- We must provide it in a commonly used, machine-readable format, and send it directly to another controller if requested.

Right to object

- We must respect the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task.
- We must respect the right of an individual to object to direct marketing, including profiling.
- We must respect the right of an individual to object to processing their data for scientific and historical research and statistics.

Rights in relation to automated decision making and profiling

- We must respect the rights of individuals in relation to automated decision making and profiling. Individuals retain their right to object to such automated processing, have the rationale explained to them, and request human intervention.

9. Subject Access Requests

What is a subject access request?

People have a legal right to access the personal data and supplementary information held about them. They can make a subject access request to the Board by email or in writing along with proof of identification.

As it had under the Data Protection Act (1998), the Board has an exemption from the subject access provisions in relation to personal data processed for the purposes of assessing any person's suitability for judicial office.

How we deal with subject access requests

This will occur without delay, and within one month of receipt of the request. Staff should be alert to subject access requests and discuss these with the DPO as soon as possible following receipt. Staff should not respond to subject access requests without first consulting the DPO.

The DPO in conjunction with the IAO, will ascertain whether the request would include any exempt supplementary information.

If the request is for a large quantity of data, we can request the individual specify the information they are requesting.

If complying with the request is complex or numerous, the deadline can be extended by two months, but the individual must be informed of the extension within one month of receipt of the request, together with the reasons for the delay. Staff must obtain approval from the DPO before extending the deadline.

We must provide an individual with a copy of the information requested, free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, we may refuse to act on the request or charge a reasonable fee. A decision to refuse to act on a request or to charge a fee should only be taken in consultation and with the express permission from the DPO.

Once a subject access request has been made, the Board or staff must not change or amend any of the data that has been requested. Doing so is a criminal offence.

Data portability requests

We must provide the data requested in a structured, commonly used and machine-readable format. This would normally be a CSV file, although other formats are acceptable. Guidance should be sought from the DPO if another format is being considered. We must provide this data either to the individual who has requested it, or to the data controller they have requested it be sent to. This must be done free of charge and without delay, and no later than within one month of receipt of the request.

10. Right to erasure

What is the right to erasure?

Subject to exemptions provided in the 2018 Act, individuals have a right to have their data erased and for processing to cease in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected and / or processed
- Where consent is withdrawn
- Where the individual objects to processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed or otherwise breached data protection laws
- To comply with a legal obligation
- The processing relates to a child

How we deal with the right to erasure

JABS is exempt from complying with the right to erasure in respect of personal data processed for the purposes of assessing an individual's suitability for judicial office. For other personal data, we can only refuse to comply with a right to erasure in the following circumstances:

- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

Staff who receive requests for erasure of personal data should first consult the DPO. If personal data that needs to be erased has been passed onto other parties or recipients, they must following consultation with the DPO be contacted and informed of their obligation to erase the data. If the individual asks, we must inform them of those recipients.

The right to object

Subject to exemptions provided in the 2018 Act, individuals have the right to object to their data being used on grounds relating to their particular situation. Staff who receive objections from data subjects should consult the DPO. Subject to exemptions, we must cease processing unless:

- We have legitimate grounds for processing which override the interests, rights and freedoms of the individual.
- The processing relates to the establishment, exercise or defence of legal claims.

We must always inform the individual of their right to object at the first point of communication, i.e. in the privacy notice. We must offer a mechanism for individuals to object online.

The right to restrict automated profiling or decision making

Subject to exemptions in the 2018 Act, we may only carry out automated profiling or decision making that has a legal or similarly significant effect on an individual in the following circumstances:

- It is based on the individual's explicit consent.
- It is otherwise authorised by law.

In these circumstances, we must:

- Give individuals detailed information about the automated processing.
- Offer simple ways for them to request human intervention or challenge any decision about them.
- Carry out regular checks and user testing to ensure our systems are working as intended.

11. Third parties

Using third party controllers and processors

As a data controller, we must have written contracts in place with any third party data controllers (and/or) data processors that we use. The contract must contain specific clauses which set out our and their liabilities, obligations and responsibilities under data protection law.

As a data controller, we must only appoint processors who can provide sufficient guarantees that the requirements of the GDPR will be fulfilled and that the rights of data subjects will be respected and protected.

Contracts

Our contracts must comply with the standards set out by the Information Commissioner's Office and, where possible, follow the standard contractual clauses which are available. Our contracts with data controllers and data processors must set out the subject matter and duration of the processing, the nature and stated purpose of the processing activities, the types of personal data and categories of data subject, and the obligations and rights of the controller.

At a minimum, our contracts must include terms that specify:

- Acting only on written instructions
- Those involved in processing the data are subject to a duty of confidence
- Appropriate measures will be taken to ensure the security of the processing
- Sub-processors will only be engaged with the prior consent of the controller and under a written contract

- The controller will assist the processor in dealing with subject access requests and allowing data subjects to exercise their rights under GDPR
- The processor will assist the controller in meeting its GDPR obligations in relation to the security of processing, notification of data breaches and implementation of Data Protection Impact Assessments
- Delete or return all personal data at the end of the contract
- Submit to regular audits and inspections, and provide whatever information necessary for the controller and processor to meet their legal obligations. Nothing will be done by either the controller or processor to infringe on GDPR.

All of the Scottish Government supplier framework agreements will have been negotiated with GDPR compliance in mind. We must be mindful that any contracts that we award that are not covered by these framework agreements must follow the above commitments to good data protection practice.

12. Data Retention

The Board will retain personal data for no longer than is necessary for the purposes of assessment and selection to judicial office, maintaining a record of its decisions and compliance with its statutory objectives. Applicants can expect that their personal data will be disposed of after one year from the conclusion of an appointment round. Some personal data will be retained permanently, namely; official appointment documentation, equality monitoring information and decisions in relation to eligibility and integrity.

13. Criminal offence data

Criminal record checks (Disclosure Scotland)

The Board must ensure that any criminal record checks are compliant with Data Protection law. Criminal record checks cannot be undertaken based solely on the consent of the subject and must be authorised by law. Staff must have approval from the DPO prior to carrying out a criminal record check.

The Board is a registered body with Disclosure Scotland. As part of the appointments process, the Board checks with Disclosure Scotland whether applicants to be recommended for appointment have criminal convictions. Disclosure Scotland applications and disclosure certificates are handled in accordance with the procedures set out in this document.

14. Audits, monitoring and training

Data audits

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant. The Board and the Secretariat must conduct a regular data audit as defined by the DPO and normal procedures.

Monitoring

Everyone must observe this policy. The DPO has overall responsibility for this policy. JABS will keep this policy under review and amend or change it as required. The Board and the Secretariat must notify the DPO of any breaches of this policy and must comply with this policy fully and at all times. Breach of this policy may constitute a disciplinary offence.

Training

The Board and the Secretariat will receive all necessary training on provisions of data protection law specific for their roles and must complete all training as required. If they move role or responsibilities, they are responsible for requesting new data protection training relevant to their new role or responsibilities.

Further information about the requirements of the GDPR is available from the Information Commissioner's Office via its website www.ico.gov.uk .

15. Reporting breaches

Any breach of this policy or of data protection laws must be reported immediately. This means that breaches must be reported as soon as we have become aware of them. JABS has a legal obligation to report any data breaches considered to be a risk to the individual to the ICO within 72 hours. It is therefore vital that the DPO is notified of breaches immediately, whether within or outside business hours.

All members of the Board and staff have an obligation to report actual or potential data protection compliance failures to the DPO. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the ICO of any compliance failures that are material either in their own right or as part of a pattern of failures

In the event of breach, Board and staff must:

- Report the breach immediately to the DPO as a security incident by email informing them what personal data has been compromised, the number of people affected and who they are and any immediate steps taken by the business area to contain the breach and recover the information

- Board and staff must not attempt to investigate the matter themselves but should immediately report any breach to the DPO. Board and staff should preserve all evidence relating to the potential personal data breach
- The DPO will decide what steps to take, including whether to inform the Information Asset Owner (IAO)
- The DPO must report serious personal data breaches to the Information Commissioner's Office within 72 hours
- Consider whether there is a high risk to the rights of the data subjects (people) involved in the breach – See Section 8

Failure to comply

We take compliance with this policy very seriously. Where an offence has been committed by a body corporate and is proved to have been committed with the consent or connivance of or to be attributable to any neglect on the part of any director, manager, secretary or similar officer of the body corporate or any person who was purporting to act in any such capacity, they as well as the body corporate shall be guilty of that offence and be liable to be proceeded against and punished accordingly.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.

Liability for Compensation

Data subjects whose rights have been infringed have the right to an effective judicial remedy against the data controller or processor responsible for the alleged breach.

Any data subject who has suffered damage as a result of infringement of the GDPR has the right to receive compensation from the controller or the processor.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the DPO.

Adopted by the Board: JUNE 2018
Next review by Quality Assurance Group/Audit and Risk Management Committee MAY 2019