Privacy Notice - Employee Data

Privacy Notice – Employee Data

To manage the organisation, deliver our services to the public and to support you, our organisation has to process personal data relating to you. This document explains how personal data relating to you is used and signposts you to how you can exercise your privacy rights.

Highlands and Islands Airports Limited (HIAL) is the controller for the uses of personal data outlined in this document and will hereafter be referred to as "we", "us" or "the organisation". In the course of performing your role, a number of different departments will process your personal data including HR, security and your department or airport.

Our Data Protection Officer can be contacted at dpo@hial.co.uk.

This privacy notice is for employees, ex-employees, agency staff, contractors, secondees, non-executive directors, job applicants, students on placement with us and volunteers. The specific information we will process about you will vary depending on your role and personal circumstances.

When appropriate we will provide a 'just in time' notice to cover any additional processing activities not mentioned in this document. Your personal information will also be processed in accordance with our organisation's policies and procedures and this is explained further below where relevant.

Your rights in relation to personal data

As an individual you have certain rights regarding our processing of your personal data, including a right to lodge a complaint with the Information Commissioner.

You have the right to:

- Be informed about the collection and use of your personal data
- Access personal data held about you and receive a copy
- Have factual inaccuracies in your personal data rectified
- In certain limited circumstances only, restrict the processing of your data or to have personal data erased, or to ask for data portability
- Object to how your personal data is being processed.

You can find independent advice about personal data rights provided by the Information Commissioner's Office.

For more information on how to exercise any of these rights, please contact the Data Protection Officer at dpo@hial.co.uk.

Sources of your personal data

We receive information about you from a range of sources:

- Directly from you
- From an employment agency
- From your employer if you are a secondee or contractor
- From referees, either external or internal
- From publicly available sources, including social media
- From security clearance providers
- From Occupational Health and other health providers
- From Pension administrators and government departments, for example tax details from HMRC
- From your Trade Union
- From providers of staff benefits
- From CCTV systems
- From network and systems logs of ICT systems which we operate as controller or which are operated on our behalf, and which you use in the course of your work.

Lawful basis for processing for personal data

Depending on the processing activity, our use of your personal data falls within different lawful grounds under the UK GDPR. These include where processing of personal data is necessary:

- For the performance of our employment contract with you (UK GDPR Article 6(1)(b))
- So we can comply with our legal obligations as your employer (UK GDPR Article 6(1)(c))
- For the performance of our public task (UK GDPR Article 6(1)(e)
- For the purposes of a legitimate interest (UK GDPR Article 6(1)(f).

Special category and criminal convictions data

Where the information we process is special category personal data, for example: your health data, information relating to some of the protected characteristics for equalities monitoring, or criminal conviction data used for checking purposes, additional lawful grounds apply where processing is necessary:

- For carrying out our obligations and exercising our rights in employment and your rights in employment and social security (UK GDPR Article 9(2)(b))
- For the establishment, exercise or defence of legal claims (UK GDPR Article 9(2)(f))
- For reasons of substantial public interest (UK GDRPR Article 9(2)(g)
- For the purposes of occupational medicine or for the assessment of working capacity (UK GDPR Article 9(2)h)
- For archiving purposes in the public interest (UK GDPR Article 9(2)(j).

In addition, we rely on processing conditions at Schedule 1 part 1 and part 2 of the DPA 2018. This relates to the processing of special category personal data for employment purposes as well as processing that is in the substantial public interest. Where we are processing criminal convictions data, we rely on processing conditions at Schedule 1 part 3

and part 4 of the DPA 2018. Our internal Data Protection Policy provides further information about this processing.

The personal data we process and why

We process the following types of information relating to colleagues and former colleagues.

Information related to your work

We use personal data to comply with the contract of employment we have with our employees, to manage the relationship with our contractors, to consider candidates for jobs or promotions, to provide you access to systems and services required for your role and to manage our human resources processes and obligations. We will also use your personal data where necessary for our functions and purposes as a Scottish public authority.

Please note that your personal data will also be processed for operational purposes and these purposes are generally defined within organisational policies and procedures rather than in this privacy notice. Occasionally we will produce additional privacy notices that relate to a specific organisational function such as driving licence checks, security, and CCTV and these are always made available on the intranet.

Personal data used for these purposes will include:

- Personal contact details such as your name, address, contact telephone numbers (landline and mobile) and personal email addresses
- Your date of birth, gender, and NI number
- A copy of your passport or similar photographic identification and / or proof of address documents
- Marital status
- Next of kin, emergency contacts and their contact information
- Employment and education history including your qualifications, job application and employment references
- Immigration status and eligibility to work information
- Location of employment
- Details of any secondary employment, political declarations, conflict of interest declarations or gift declarations
- Security clearance details including basic checks and higher security clearance details according to your job
- Any criminal convictions that you declare to us
- Your responses to staff surveys and consultations where this data is not anonymised
- Information relating to you recorded as part of our business correspondence and processes
- Recordings of phone calls or meetings
- Any content featuring you produced for use on our website or social media such as videos, authored articles, blog posts and speech transcripts.

Salary, pension and loans

We process this information for the payment of your salary, pension, and other employment related benefits to meet our legal obligations and our contractual obligations to you. We also process it for the administration of statutory and contractual leave entitlements such as holiday or maternity leave.

- Information about your job role and your employment contract including your start and leave dates, salary (including grade and salary band), any changes to your employment contract, working pattern (including any requests for flexible working)
- Details of your time spent working and any overtime, expenses or other payments claimed, including details of any loans such as for travel season tickets or cycle-to-work schemes
- Details of any leave including sick leave, holidays, special leave etc
- Pension details including membership of both state and occupational pension schemes (current and previous)
- Your bank account details, payroll records and tax status information
- Details relating to Maternity, Paternity, Shared Parental and Adoption leave and pay. This includes application forms, matching certificates and any other relevant documentation relating to the nature of the leave you will be taking.

Your performance and training

We use this information to assess your performance, to conduct pay and grading reviews and to deal with any employer-employee related disputes. We also use it to meet the training and development needs required for your role.

- Information relating to your performance at work such as performance and development reviews, probation, promotions, objectives
- Grievance and dignity at work matters and investigations to which you may be a party or witness
- Disciplinary records and documentation related to any investigations, hearings and warnings/penalties issued
- Whistleblowing concerns raised by you, or to which you may be a party or witness
- Information related to your training history, attendance and performance in training courses and development needs
- Audio and video from any training sessions you attend that are being recorded where you are identifiable from the recording.

Monitoring

We use information to assess your compliance with corporate policies and procedures and to ensure the security of our premises, ICT systems and employees including information derived from monitoring ICT acceptable use standards, and CCTV images.

All of our ICT systems, Electronic Document and Record Management systems and the swipe access system for the entry and exit of our premises are auditable and can be monitored, though we don't do so routinely. We are committed to respecting individual users' reasonable expectations of privacy concerning the use of our ICT systems and equipment. However, we reserve the right to log and monitor such use in line with our Acceptable Use Policy.

Any targeted monitoring of staff will take place only within the context of our disciplinary procedures.

Counter-fraud

We will carry out checks as necessary to prevent fraud and ensure appropriate use of public funds. Where necessary, we will share information about suspected fraud with Audit Scotland, Police Scotland, and other relevant statutory agencies.

We participate in the National Fraud Initiative, providing payroll and trade creditor information to Audit Scotland to allow data matching for the detection of fraud under the Public Finances and Accountability (Scotland) Act 2000. Matched data is also shared with the Cabinet Office at UK level. We may receive reports of matches found in the NFI exercise to investigate further.

For more information see the National Fraud Initiative privacy notice.

Health and wellbeing and other special category data

We use the following information to comply with our legal obligations, for equal opportunities monitoring, and to ensure the health, safety and wellbeing of our employees:

- Health and wellbeing information either declared by you or obtained from health checks, eye examinations, occupational health referrals and reports, sick leave forms, health management questionnaires or fit notes
- Accident records if you have an accident at work
- Details of any desk audits, access needs or reasonable adjustments
- Information you have provided regarding protected characteristics as defined by the Equality Act and for the purpose of equalities monitoring. This includes racial or ethnic origin, religious beliefs, disability status, and gender identification, marital status, and sexual orientation, and may be extended to include other protected characteristics
- The results of drug and alcohol testing
- Information you provide to any of our equality and diversity networks
- Information you may choose to provide in complete confidence to our Wellbeing Champions, and statistical data on the types of concerns raised with our Wellbeing Champions.

During your employment you may be referred to occupational health following a request to HR by you or your line manager. This may result in a face-to-face consultation, a telephone appointment with an occupational healthcare professional and/or a medical report from a GP or specialist. The information you provide will be held by our occupational healthcare provider, who will give us a fit to work certificate or a report with recommendations. The occupational health provider or other clinician may ask for your consent to share relevant information relating to your health and fitness to work.

Please note that we do not use consent as the lawful basis for processing health and fitness to work data.

Security

Basic security checks and / or advanced checks will be carried out based on your role in line with HIAL's policies. The relevant privacy notices can be found on the intranet and the HIAL website under the privacy policies section.

Where relevant to the role, job applicants are required to complete a Basic Disclosure check via Disclosure Scotland or the equivalent in other countries.

All staff are all issued with a security pass that displays your name, job title, reference number, photograph, and expiry date. Staff pass details and data on the use of the pass to enter and leave the building are held securely and can only be accessed by a restricted number of authorised staff.

Whistleblowing

We have a policy and procedure in place to enable current staff and ex-employees to have an avenue for raising concerns. Information in this context is processed by us because it is necessary for our compliance with our legal obligations under the Public Interest Disclosure Act 1998.

Although every effort will be taken to restrict the processing of your personal data and maintain confidentiality whether this is possible will be dependent on the nature of the concern and any resulting investigation.

How long we keep your personal data

For information about how long we hold your personal data, see our retention schedule, which is available on the information management team site, on the HIAL intranet.

When you leave the organisation, HIAL has a legitimate interest in retaining your personal data after your contract has concluded, and the length of time information is held is also in the retention schedules referenced above.

Recipients of your personal data

In some circumstances, such as under a court order, we are legally obliged to share information. We may also share information about you with third parties including our data processors, training providers, government agencies and external auditors. For example, we may share information about you with HMRC for the purpose of collecting tax and national insurance contributions.

Additionally, we are required under the Public Records (Scotland) Act 2011 to transfer records to National Records of Scotland for permanent preservation. Some of these records may include the personal data of our current and former employees. Full consideration will be given to Data Protection and Freedom of Information legislation when making decisions about whether such records should be open to the public.

The recipients or categories of recipients of your personal data are listed below:

- HMRC and other government agencies that HIAL is required to pass data to. This may include Audit Scotland, the Cabinet Office and the Home Office

- National Records of Scotland
- Payroll services providers
- Recruitment agencies and systems, and other IT systems providers that help us manage employee records
- Pension scheme administrators
- Online test providers
- Occupational Health provider
- Staff benefits providers. You will usually be required to opt into these schemes, unless it is something for all employees. This will include schemes such as cycle-to-work and childcare vouchers as and when HIAL offers these
- Training providers both online and face to face in a physical location
- Document management services including scanning, storage and destruction
- Staff survey tool providers
- IT ticketing software
- Data Protection Officer, where the role is outsourced
- Under certain circumstances, we will share your personal data with professional advisers including lawyers, bankers, auditors, and insurers based in the UK who provide consultancy, banking, legal, insurance and accounting services to us.

Please note that some of the systems above that offer self-service use cookies which are all essential for system functionality. HIAL does not collect any additional data using cookies. Where a system provider collects personal data using cookies for their own purposes, they should always provide a privacy notice to you.

Other than described above, HIAL will never pass personal information to any other third party, unless there is a statutory requirement to do so, or the processing is otherwise lawful.

Disclosures under Freedom of Information

As a public authority we receive information requests under the Freedom of Information (Scotland) Act 2002 or Environmental Information (Scotland) Regulations 2004. Sometimes personal data relating to staff (including agency and temporary staff) falls within the scope of a request and we must consider whether to disclose the personal data as part of our response.

We will normally disclose non-sensitive work-related information about staff in a public-facing role. We may also disclose information about staff members whose work is purely administrative if their names are routinely sent out externally. This information is published where there is a clear legitimate interest for HIAL to do so.

It is less likely that information about those who do not deal directly with the public in an operational capacity will be disclosed. Senior management may have more information disclosed about them, such as photographs and biographical detail, due to their position in the organisation.

We will consider withholding information if we think that it will prejudice the rights and safety of our staff, irrespective of grade or position.

Requests for references

If you have left or are thinking of leaving, we may be asked by your new or prospective employers to provide a reference. For example we may be asked to confirm the dates of your employment or your job role. We will usually provide information where it is limited to basic details.

International transfers of personal data

We don't routinely transfer colleague personal data overseas but when this is necessary, we will ensure that we have appropriate safeguards in place and that this is done transparently.