

# Data Protection Policy

## Purpose

1. This policy is aimed at ensuring compliance with the Data Protection Act 1998 (DPA).

## Scope

2. This policy applies to all established and temporary employees who work under a contract of service and all agency staff, casual workers, work experience/placement students, contractors and consultants who work under a contract for service.

## Policy Statement

3. The Office of Rail Regulation (ORR) not only intends to comply with its obligations under the DPA, but also wishes to assure both employees and all other persons about whom it retains personal data, that this will be processed in compliance with the DPA and any Codes of Practice issued by the Information Commissioner and will be stored in a secure, confidential and appropriate manner. The data will only be stored whilst it is relevant and will not be disclosed to any person without the employee's personal written authority or unless required by law e.g. personal data required by the Inland Revenue under the Taxes Management Act 1970.

4. To this end, the ORR is committed to upholding the following principles: (a) personal data will be processed fairly and lawfully;  
(b) the amount of personal data held will be adequate, relevant and not excessive in relation to the purposes for which it is held;  
(c) personal data will be accurate and, where necessary, kept up to date;  
(d) personal data will be obtained only for the specified and lawful purposes and will not be further processed in any manner incompatible with the purpose(s);  
(e) personal data will only be held for so long as it is necessary to enable those specified and lawful purposes to be achieved;  
(f) any individual about whom personal data is retained or is being processed will be informed by the ORR of:
  - (i) the purpose for which this is being done;
  - (ii) to whom such data may be disclosed;
  - (iii) the source of such data and who will have access to it, in an intelligible form upon request; and

- (iv) how to have such data corrected or erased, where appropriate.
  - (g) personal data will be secured against unauthorised or unlawful processing, accidental loss, destruction or damage;
  - (h) personal data will only be transferred to a country outside the European Economic Area if that country's laws provide similar protection to the individual concerned or if such transfer is necessary for the performance of any obligations under the contract of employment or for any other lawful reason.
5. The ORR will only process "sensitive" and other "personal data" relating to an individual if it is required in connection with the employment of that individual by the ORR and/or if required by law.
6. The person responsible for the application of this policy is the head of information management.

## Responsibility

7. All those persons referred to within the scope of this policy are required to adhere to its terms and conditions. They must understand that this policy is also incorporated into their contract of employment.
8. Individual managers are responsible for ensuring that this policy is applied within their own area. Any queries on the application or interpretation of this policy should be discussed with the head of information management prior to any action being taken.

## Background information to the Data Protection Act

9. The DPA regulates the way we handle information about living individuals. It does this by prescribing a set of rules known as the "data protection principles". These principles are designed to ensure that there are certain safeguards in place which protect individuals' privacy. It also gives individuals on whom we hold information certain rights. This means that individuals can request to see their personal data (the right of subject access); correct any inaccuracies they discover in their personal data; and object to what is being done with their personal data if this is causing them unwarranted and substantial damage or distress. These rights are all part and parcel of the right to respect for the privacy of personal information.

## Definitions

10. The following terms are used throughout this policy and its application. These definitions comply with those used within the DPA. Each term is therefore defined as follows:
- (a) "**Data**" is information which:
    - (i) is processed by equipment operating automatically in response to instructions given for that purpose;
    - (ii) is recorded with the intention that it should be so processed; and/or
    - (iii) is recorded as part of a relevant filing system.
  - (b) "**Relevant filing system**" means any set of information, which is not processed by means of equipment, but is structured in such a way that specific information relating to a particular individual is readily accessible.
  - (c) "**Personal data**" is data consisting of information which relates to a living individual

who can be identified from that information (or from that and other information in possession of the data controller), including any expression of opinion about the individual and any indications of the intention of the data controller or any other person in respect of that individual.

- (d) **“Sensitive personal data”** means personal data consisting of information as to racial or ethnic origins; political, religious or other opinions/beliefs of a similar nature; physical or mental health; sexual life; criminal offences or alleged criminal offences and past sentences; and whether he/she is a member of a trade union.
- (e) **“Data Controller”** The “Office of Rail Regulation” is the data controller, which means that data protection responsibility and legal liability rests with the ORR itself.
- (f) **“Data Subject”** is an individual who is the subject of personal data.
- (g) **“Processing”** is obtaining, recording, holding or carrying out any operation on data; such as the organisation, adaptation, alteration, retrieval, disclosure, dissemination, rearranging or destruction of the information or the data.
- (h) **“Data Processor”** is any person who processes data on behalf of the data controller.

## Exemptions

11. Specific sets of information are exempt from the DPA and are therefore excluded from the detailed provisions of this policy but in certain instances the spirit of the policy will be maintained, so far as is reasonably practicable. The main exemptions regarding employment records are:

- (a) information which the ORR is required by law to make public e.g. personal data requested by the Inland Revenue under the Taxes Management Act;
- (b) information which the ORR is required to make available in connection with legal proceedings e.g. personal information relating to an employment tribunal;
- (c) personal data processed for the prevention of crime or prosecution of offenders or for the collection of tax;
- (d) confidential references prior to being given by the ORR (see paragraph 32 for further detail);
- (e) information relating to Crown employment and Crown or Ministerial appointments;
- (f) management forecasts/management planning e.g. data can be withheld if supplying it would prejudice the employer’s business but only whilst the planning/forecasting is in progress, such as planning for redundancies. Once the process is completed and decisions and actions have been taken any personal data are subject to disclosure;
- (g) information relating to negotiations e.g. pay negotiations, to the extent that such information would prejudice negotiations.

12. With the exception of the above no personal data, whether held on computer or in hard copy, will be released to any individual or organisation outside of the ORR. Within the ORR the data will only be released as appropriate and in accordance with this policy.

## Consent to process data

13. The ORR will only collect personal information about employees when that information is required for a legitimate business or legal reason. Under normal circumstances personal data

will only be obtained from the employee or with his/her consent. Where it is appropriate to consult sources other than the employee (e.g. for references) then he/she will be informed of that fact.

14. Personal data may only be processed if one of the following conditions is met:

- (a) the data subject has given his/her consent; or
- (b) the processing is necessary for the performance of a contract (such as an employment contract) or for entering into a contract; or
- (c) the processing is necessary in order to comply with any legal obligation to which the ORR or the employee is subject; or
- (d) the processing is necessary in order to protect the vital interests of the employee; or
- (e) the processing is necessary for the administration of justice or for other legal reasons; or
- (f) without prejudice to the data subject's rights, freedoms or legitimate interests when the processing is necessary for the purposes of legitimate interests pursued by the ORR or by the third party to whom the data is disclosed (such as where there may be a business transfer or merger).

15. In order to process personal data in accordance with the DPA, the ORR requires employees to sign the Consent Form (attached as Annex A) for the processing of data for all purposes relating to employment. The Consent Form will be issued to all potential employees along with their Statement of Terms and Conditions of Employment, at the time of the written offer of employment with the ORR.

## Retention of personal data

### Storage

16. All documentation relating to employment is contained in hard copy, in an individual file for each employee, within HR. Managers must not hold these or duplicate files locally. The only exceptions to this principle are:

- (a) Current performance and development review documentation, sickness records and any notes relating to conduct and performance problems – kept by managers within the employee's directorate.
- (b) Training and Development records – kept by the learning and development adviser within the employee's directorate.
- (c) Medical Reports and Health Screening Assessments – kept by Everwell, our Occupational Health provider with copies kept in the HR team as appropriate; and
- (d) Payroll and Pension information – kept by Logica and the ORR Finance team. (e) Union Membership Records – kept by the ORR union representatives.

17. Hard copy records may not be removed from the place in which they are kept without the prior authorisation of the responsible person named above.

18. In addition, HR stores and processes sensitive and other personal data electronically on MyHR, the Human Resources database. This system is managed and administered by members of HR and the Information Systems team are responsible for system

support.

19. It is important that personal data is kept protected at all times. This includes both paper and electronic material. Relevant personal data, as highlighted below, should therefore always be protectively marked. Data is personal when it relates to an identifiable living individuals.

20. Following Cabinet Office guidelines, the following types of personal data should always be used with a protective marking:

- (a) One of more pieces of information which can be used along with public domain information which can be used along with public domain information to identify an individual. This includes: name; addresses (home, business or both); postcode; email address; telephone numbers; driving licence number; and date of birth

Combined with

- (b) Information about that individual, release of which is likely to cause harm or distress. This includes: 'sensitive' personal data as defined by the DPA. This is information about race/ethnic origin; political opinions; religious beliefs; trade union membership; physical/mental health; sexual life; commission/alleged commission of an offence and any proceedings for an offence or alleged offences. It also includes DNA or fingerprints; bank, financial or credit card details; mother's maiden name; NI number; tax, benefit or pension records; health records; and employment records (including appraisals).

### **Protectively marking personal data**

21. The following protective markings are used for handling personal data (a descriptor must always be used with the PROTECT marker):

- (a) PROTECT – PERSONAL (refers to material only to be seen by the addressee)
- (b) PROTECT – STAFF (includes references to named or identifiable staff or personal confidences entrusted by staff to management).

22. Follow the instructions for handling PROTECT material, as laid out in ORR's security manual part 2: information security, for handling and protecting personal data.

### **Retention Period**

23. The amount of data retained will be regularly reviewed and reduced in line with ORR's retention and disposal policy. The relevant time periods are shown in Annex B.

### **Accuracy of Information**

24. The ORR will take such reasonable action as is necessary to ensure the accuracy of information. Data is deemed to be inaccurate if it is either incorrect or misleading as to any matter of fact.

25. HR will provide employees with a copy of the personal details held on the HR database, on an annual basis, in order that they may update the data or raise queries regarding the content of the information.

26. In addition to the requirement for accuracy from a data protection perspective, information held is important for the correct administration of employee benefits and other details, such as telephone number and contact details of the next of kin are also needed for health and safety reasons. For these and other employment reasons, it is a condition of employment that any change in an employee's circumstances must be notified by the individual to HR as soon as is practicable, so that records can be updated.

## Access to personal data

27. All employees may request to see and have a copy of the sensitive and other personal data held by the ORR other than for:

- (a) management information if the release of such information could prejudice the ORR's business interests;
- (b) information relating to negotiations with the ORR if the disclosure would prejudice those negotiations;
- (c) information required for the purposes of management forecasting and succession planning if the release of such information could prejudice the conduct of the business; or
- (d) confidential references given by the ORR before they are provided to a third party.

28. Employees do not have the right of access to information relating to another individual, or to information identifying that individual as the source of the information sought by the employee, unless that individual has given his/her consent for the information to be disclosed or unless it can be taken, in all circumstances, that the individual has dispensed with their consent. For example, employees should be aware that, in addition to members of the department in which the information is held, a manager with direct and/or indirect line responsibility for their work activities may, in certain circumstances, also have access to their personal data.

29. Any employee who is concerned as to the nature or existence of any personal data may request access to the personal data (other than as stated above) held by the ORR by applying in writing to the head of information management and specifying the information that is requested. Annex C may be used for this purpose. The ORR will supply the information within 40 calendar days of receiving a request but it should be noted that the original copy of the information held by the ORR must not be removed from its normal place of storage. The data requested will be sent to the individual by post unless the employee wishes to view their entire personal file. In this situation a member of HR will accompany the employee whilst viewing the information.

30. Similarly, managers may not remove the original copy of personal information held by the ORR about their staff, from its normal place of storage, without the prior authorisation of the relevant member of HR or head of information management and only after providing a written acknowledgement of the receipt of the information.

## Personal data usage

31. Sensitive and other personal data collected for employment purposes will only normally be used for such purposes. No important decisions will be made with regard to any individual using, or referring to, data that was collected for any other purpose.

32. All forms supplied by the ORR to be completed by employees or potential employees for employment purposes will include an explanatory statement regarding the purpose for which the information is to be used, where the information will be kept and for how long, and who will have access to the information.

33. Disclosure of information will only be permitted as referred to in this policy or if the individual has provided his/her consent.

34. Where the processing of data by automated means is likely to constitute the sole basis for any decision affecting the individual, such as is the case with certain psychometric tests, the individual will be informed of the logic involved in the decision making process.



35. Personal data will not be transferred to a country outside the European Economic Area without the individuals consent to the transfer of the data.

## References

36. Confidential references provided by the ORR to another organisation are exempt from the access provisions of the DPA prior to their issue. This includes references supplied for the following purposes:

- (a) education;
- (b) training;
- (c) employment; or
- (d) provision of any service.

37. This means that employees may not see a reference supplied by the ORR before it is sent. However, the exemption is not applicable, and employees may have access, to references once they are received by the ORR and/or to references sent by the ORR once they have been received by the intended third-party.

38. The employee's permission for the ORR to supply a reference must be obtained before any reference can be given. All persons voluntarily leaving the employment of the ORR will therefore be asked to confirm their agreement to such references being supplied to prospective future employers during their exit interview (see ORR Exit Policy for details). Similarly, the written consent of an employee must be provided before references will be supplied to Banks, Building Societies or other organisations.

39. All references relating to past and current employees must be written by a member of the Human Resources department, who will discuss the detail with the appropriate manager of the employee when necessary. Factual references will be supplied by the ORR which confirm such details as length of service, position(s) held, reason for leaving, final salary and, if requested, attendance levels.

40. Should a manager receive a request for a reference for a past or current employee they must forward the request to Human Resources. If they wish to provide a "character reference" they must explicitly state that the reference is a personal reference from the individual concerned; it must not be sent on ORR letter- head stationery and should not in any circumstances be considered to be the views or opinion of the ORR.

## Applications for vacancies in other Government Departments

41. Should a member of ORR staff apply for a vacancy in another government department they may be asked to provide the recruiting department with their last 3 years' appraisal reports and their sickness record for the last 12 months. HR will only provide this information with the written permission of the employee.

## Medical records

42. For details of the right of access to any medical report prepared by a medical practitioner relating to employment, the employee must either request details from the medical practitioner concerned or from HR. Details of employees' rights under the Medical Reports Act 1988 are specified prior to any pre-employment or employment medical being requested.

43. Any employee, or any person authorised in writing by that employee, may also apply to receive details of occupational health material held by ORR about the employee. Similarly, should ORR wish to apply for details of an employee's medical records retained by their general practitioner the employee's consent will be requested beforehand.

44. If an employee is requesting access to reports prepared for ORR by its occupational health advisers, ORR is required to request permission to disclose these reports from the provider. This is in line with our obligations under the Data Protection Act 1998 and the Data Protection (Subject Access Modification) (Health) Order 2000 that release of medical information must be through the consent of a qualified health professional.

## **Transferring to or from another Government Department**

45. When a member of staff transfers to ORR from another Government Department, the files are subject to the ORR Data Protection Policy (ie. this policy).

46. When a member of staff transfers from ORR to another Government Department, their files will be transferred with them and they are subject to the Data Protection Policy of their new department.

## **Maintaining this policy**

47. The head of information management has responsibility for ensuring the maintenance, regular review and updating of this policy.



## ANNEX A

# DATA PROTECTION ACT CONSENT FORM

## DATA PROTECTION ACT 1998

In order to comply with the Data Protection Act 1998, ORR must obtain permission to hold and use personal information about individuals that could be considered sensitive.

The purposes for which sensitive personal data will be held and processed are listed below:

- administering and maintaining personnel records;
- paying and reviewing salary and other remuneration and benefits;
- providing and administering benefits;
- undertaking performance appraisals and reviews;
- recording and managing training;
- maintaining sickness and other absence records;
- taking decisions as to my suitability and fitness for work at the ORR;
- providing references and information to future employers, and if necessary, governmental and quasi-governmental bodies for social security and other purposes and HMRC;
- processing information regarding equality of opportunity and treatment of employees in line with the ORR's equality and diversity policies.

**I have read the Data Protection Policy and understand that sensitive personal data relating to me will only be used for the purposes set out in the statement above, and my consent is conditional upon ORR complying with the obligations and duties under the Data Protection Act 1998.**

Name..... Signed.

..... Date.....

**Please sign, date and return this form to HR for placement on your personal file**

## ANNEX B

### RETENTION OF RECORDS

HR policy and procedures incl Equality, Diversity	P	Including superseded policies
Recruitment documentation	CY + 2Y	Includes application forms, list of applicants, internal job application forms & board papers
Discipline/Grievance documentation	Refer to current HR policy	
Personnel files on ORR staff including contracts, T&Cs, appraisals	T + 6Y	T = termination of employment
Personnel – Occupational health issues	T + 40Y	T = termination of employment
Personnel – Pensions records	T + 6Y	T = final payment of pension i.e. at employees dependent's death
Payroll	CY + 10Y	
Pension scheme records	P	Includes documentation setting out the terms of the pension scheme
Employee relations and Union agreements	P	SRG and union relations

NB: P = 30 years under the terms of the Public Records Act 1958

## ANNEX C

### Data protection act 1998 – request for personal data

- The Data Protection Act 1998, gives rights to individuals in respect of personal data held about them by others.
- Please complete this form if you wish to access personal data held by ORR.
- Please provide all of the information requested in this form.
- We will comply with your request within 40 calendar days of receipt of a fully completed form as required by the Act.

<b>Full Name:</b>	<b>Directorate:</b>
<b>Pay Reference:</b>	
<b>Please give details below of the personal data you wish to access:</b>	
<b>The data will be sent to you by post unless, exceptionally, we contact you to suggest another way to provide access. Please give us the full address you wish us to use:</b>	
<b>Please let us know whether you have any special needs as to how the data should be provided and we will do our best to accommodate them:</b>	
<b>Signed:</b>	<b>Date:</b>

**Please return the completed form to the head of information management**

## ANNEX D

### Do's and Don'ts guide for managers on employee records and data protection

Do	Don't
Keep only current PDR information, sickness records and in exceptional circumstances notes relating to performance and conduct, in your own department. This information should be kept confidentially in a locked drawer or cabinet or if computerised ensure it is protected.	Keep duplicate HR files, ensure any information held on an employee which does not relate to their current PDR or conduct/performance/sickness problems is sent to HR for storage
Ask permission from a Member of HR to remove any information from an employees personal file and provide a written acknowledgement of receipt	Remove personal files or information from HR without permission.
Forward all requests for references to HR	Give written or telephone references for any employee.
If you wish to provide a "character reference" for an employee then you must explicitly state that the reference is a personal reference from you; it must <u>not</u> be sent on ORR headed paper and should not in any circumstances be considered the views or the opinion of ORR	Give "character references" on ORR letter-head stationary
Contact a member of HR for guidance where necessary	