pirc people plan

DATA PROTECTION POLICY

pirc

Police Investigations & Review Commissioner

CONTENTS

1. Introduction

The Police Investigations & Review Commissioner (PIRC) is a data controller in terms of the Data Protection Act 1998 ("DPA"). As a registered data controller, the PIRC has a statutory duty to comply with the provisions of the DPA.

The DPA operates in two ways. Firstly, it provides that anyone handling personal information must comply with the eight data protection principles laid down in the DPA. Secondly, it provides individuals with rights in relation to information which relates to them and places duties on data controllers to uphold these rights.

We are required to maintain certain personal data about individuals for the purposes of satisfying our operational and legal obligations. We recognise the importance of correct and lawful treatment of personal data as it helps to maintain confidence in our organisation and to ensure efficient and successful outcomes when using this data.

The types of personal data that we may process include information about current, past and prospective employees; applicants and enquirers; suppliers and other organisations with which we have dealings.

Personal data may consist of data kept on paper, computer or other electronic media; all of which is protected under the Data Protection Act 1998.

This policy summarises the key concepts contained in the DPA and the responsibilities of the PIRC as a data controller under the DPA.

2. DPA Principles and Definitions

We endorse and adhere to the eight principles of the Data Protection Act which are summarised below. Data must:

1. Be processed fairly and lawfully processed
2. Be obtained for a specified and lawful purpose
3. Be adequate, relevant and not excessive for those purposes.
4. Be accurate and, where necessary, kept up to date.
5. Only be kept for as long as is necessary for the purpose for which it was obtained.
6. Be processed in accordance with the data subject's rights.
7. Personal data must be secure
8. Not be transferred to other countries without adequate protection

Employees of PIRC who obtain, handle, process, transport and store personal data for us must adhere to these principles at all times.

3. Types of Data

The DPA lays down conditions for the processing of any personal data, and makes a distinction between personal data and "sensitive" personal data.

Personal data is defined as data relating to a living individual who can be identified from that data; or from that data and other information which is in the possession of, or is likely to come into the possession of the data controller and includes an 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.

Sensitive personal data is defined as personal data consisting of information regarding an individual's racial or ethnic origin; political opinion; religious or other beliefs; trade union membership; physical or mental health or condition; sexual life; or criminal proceedings or convictions.

4. Handling of Personal/Sensitive Information

All staff should be aware that the PIRC is a data controller under the DPA, understand the key provisions of the DPA and the PIRC' responsibilities as a data controller, and should take responsibility for ensuring that their actions are in compliance with the DPA in their handling of personal information. As a data controller, the PIRC will be processing sensitive personal data as part of its functions.

The PIRC will, through appropriate management and the use of strict criteria and controls:

- observe fully the conditions concerning the fair collection and use of personal information
- specify the purpose for which information is used
- collect and process information only to the extent that it is needed to fulfil operational needs or legal requirements
- endeavour always to ensure the quality of information used
- not keep information for longer than required operationally or legally
- always endeavour to safeguard personal information by physical and technical means (i.e. keeping paper files and other records or documents containing personal/sensitive data in a secure environment;
- protecting personal data held on computers and computer systems by the use of secure passwords, which where possible, are changed periodically and ensuring that individual passwords are not easily compromised)
- wherever possible staff access to printers will be restricted to secure printing where allocated passwords are used to print materials from the printer to which they are sent
- ensure that personal information is not transferred abroad without suitable safeguards
- ensure that the lawful rights of people about whom the information is held can be fully exercised

In addition, the PIRC will ensure that:

- there is someone with specific responsibility for data protection in the organisation (the designated Data Controller) - currently the Head of HR & Corporate Services (HHRCS)
- all employees managing and handling personal information understand that they are contractually responsible for following good data protection practice
- all employees managing and handling personal information are appropriately trained and supervised to do so
- a clear procedure is in place for anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, and that such enquiries are promptly and courteously dealt with
- methods of handling personal information are regularly assessed and evaluated

- data sharing is carried out under a written agreement, setting out the scope and limits of the sharing, except in situations where legislation allows sharing of information within the functions of the PIRC.
- any disclosure of personal data will be in compliance with approved procedures

5. Access to Personal Data

Subject Access Requests

The DPA gives individuals the right to make a request, in writing, for a copy of the personal data which the PIRC holds about them. This is known as a '*subject access request'*.

If any person at the PIRC receives what appears to be a subject access request, the request should be passed in the first instance to the Information Officer who is responsible for responding to Subject Access Requests on behalf of the HHRCS. The PIRC has 40 calendar days from the date of receipt to respond to subject access requests under the DPA, so such requests should be date stamped upon receipt and passed immediately to the Information Officer.

We reserve the right to charge the maximum fee payable for each subject access request, currently set at £10. Under normal circumstances this will only be requested when an individual has already requested their personal data on two previous occasions, and had this provided without charge. Thereafter a charge of £10 will be made for each and any future request.

Where the PIRC considers that it wishes to charge the statutory fee to meet the terms of the request, the individual requesting the information should be informed promptly and the 40 day period for response commences upon receipt of the fee.

Personal information will only be released to the individual to whom it relates. The disclosure of such information to anyone else without their consent may be a criminal offence. Any employee who is in doubt regarding a subject access request should check with the Information Officer.

We aim to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days of receipt of a written request unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the individual making the request.

Some information requested by individuals may be exempt from release. The DPA contains a number of clearly defined exemptions, for example personal data processed for the prevention and detection of crime or the apprehension of prosecution of offenders.

If the PIRC does not hold any personal information about an individual who has made a subject access request, the individual will be told this.

If personal details are inaccurate, they will be amended upon request. If by providing this information we would have to disclose information relating to or identifying a third party, we will only do so provided the third party gives consent, otherwise we may edit the data to remove the identity of the third party.

6. Employee Responsibilities

All employees must ensure that, in carrying out their duties, the PIRC is able to comply with its obligations under the DPA. In addition, each employee is responsible for:

- checking that any personal data that he/she provides to us is accurate and up to date
- informing us of any changes to information previously provided, e.g. change of address
- checking any information that we may send out from time to time, giving details of information that is being kept and processed
- if, as part of their responsibilities, employees collect information about other people or about other employees they must comply with this policy.

Information stored on enquirer/applicants should be reviewed regularly to ensure it is accurate and up to date. All documents, whether hand written or stored in emails (current or deleted) are potentially disclosable in the event of a subject access request.

7. Data Security

Personal data held by the PIRC which relates to others should be kept in accordance with an appropriate level of security, taking into account the nature of the information and the harm that might result from unauthorised disclosure.

The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage, and both access and disclosure must be restricted.

All employees are responsible for ensuring that any personal data which they hold is kept securely and that personal information is not disclosed either orally, in writing or otherwise to any unauthorised third party.

8. Offences under the DPA

The ICO have powers to administer fines of up to £500,000 depending on the severity of the offence. The following offences set out in the DPA attract both corporate culpability and individual personal culpability, where the data controller is a body corporate:

- Processing without registration
- Failure to notify the Information Commissioner of changes to the notification register entry
- Failure to comply with written request for particulars
- Failure to comply with an enforcement notice/information notice/special information notice
- Knowingly or recklessly making a false statement in compliance with an information notice or special information notice
- Intentional obstruction of, or failure to give reasonable assistance in, execution of a warrant
- Unlawful selling of personal data
- Enforced subject access

The DPA also creates one offence which attracts individual personal culpability only. This is the offence set out in section 55(1) of the DPA, and relates to the unlawful obtaining, disclosing or procuring of personal data.

9. Publication of Information

Information that is already in the public domain is exempt from the 1998 Act. This would include, for example, information on employees contained within externally circulated publications.

Any individual who has good reason for wishing details in such publications to remain confidential should contact the Head of HR & Corporate Services.

10. Subject Consent

The need to process data for normal purposes will be communicated to all data subjects as appropriate.

Our contracts of employment provide the consent of employees to the processing of personal data for the purposes of administering, managing and employing our employees. This includes: payroll, benefits, medical records, absence records, sick leave/pay information, performance reviews, disciplinary and grievance matters, pension provision, recruitment, family policies (maternity, paternity, adoption etc) and equal opportunities monitoring.

In some cases, if the data is sensitive, for example information about health, race or gender, express consent to process the data will be obtained. Such processing may be necessary to carry out the functions of the PIRC and to comply with some of our policies, such as health and safety and equality and diversity.

Information about an individual will only be kept for the purpose for which it was originally given. Employees and managers must not collect or store data which is not necessary or which is to be used for another purpose.

11. Retention and Disposal of Data

Personal data should not be retained by the PIRC for longer than is required for the purposes for which it was collected.

Information will be kept in line with our Records Management Policy. The Information Officer is responsible for ensuring that information is not kept for longer than necessary.

Documents containing any personal information will be disposed of securely, and paper copies will be shredded.

12. Registration

The PIRC is registered in the Information Commissioner's public register of data controllers.

The Data Protection Act 1998 requires every data controller who is processing personal data to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence.

The Head of HR & Corporate Services is our designated Data Controller and is responsible for ensuring compliance with the Data Protection Act, for notifying and updating the Information Commissioner of our processing of personal data, and for the monitoring and implementation of this policy on behalf of PIRC.

13. Implementation, Monitoring and Review of this Policy

The HHRCS has overall responsibility for implementing and monitoring this policy, which will be reviewed on a regular basis following its implementation (at least annually) and additionally whenever there are relevant changes in legislation or to our working practices.

Any queries or comments about this policy should be addressed to the HHRCS.

This policy indicates how the PIRC intends to meet its legal responsibilities for data protection. Any breach will be taken seriously and may result in formal disciplinary action. Any employee who considers that the policy has been breached in any way should raise the matter with his/her line manager or the HHRCS.

14. Communication & Contacts

This policy will be shared with all PIRC staff and may be published for access by prospective candidates on our website.

Queries should be addressed to:

Head of HR & Corporate Services
Hamilton House
Hamilton Business Park
Hamilton
ML3 0QA

Phone: 01698 542900

Email: enquiries@pirc.gsi.gov.uk

15. Benchmarks Used in Policy Formulation

- Scottish Government
- ACPOS
- Previous PCCS Policy
- Risk Management Authority

16. Review of Policy

This Policy is a formal PIRC policy and will be reviewed by the Head of Department Group on an annual basis.

Version Control Data

Title:	Data Protection Policy
Author:	Janice Carter, Information Officer
Approver:	Les Common, Head of HR & Corporate Services
Version Number:	Version 3
Date of Approval:	February 2017
Summary of last modification:	General check for any changes which might affect policy.
Modified by:	Janice Carter
Next review date:	February 2018